Research, Society and Development, v. 9, n. 2, e178921979, 2020
(CC BY 4.0) | ISSN 2525-3409 | DOI: http://dx.doi.org/10.33448/rsd-v9i2.1979

Vulnerabilidades em redes Wi-Fi de instituições de ensino superior: um estudo de múltiplos casos

Higher education institution Wi-Fi network vulnerabilities: a multiple case study

Vulnerabilidades en la red Wi-Fi de la institución de educación superior: un estudio de caso múltiple

Recebido: 01/11/2019 | Revisado: 01/11/2019 | Aceito: 02/12/2019 | Publicado: 11/12/2019

Davis Anderson Figueiredo
ORCID: https://orcid.org/0000-0003-2267-3583
Universidade Fumec, Brasil
E-mail: davis.figueiredo@fumec.br
Rodrigo Moreno Marques
ORCID: https://orcid.org/0000-0002-6320-4874
Universidade Fumec, Brasil
E-mail: rodrigo.marques@fumec.br
Henrique Cordeiro Martins
ORCID: https://orcid.org/0000-0002-8064-7386
Universidade Fumec, Brasil
E-mail: henrique.martins@fumec.br
João Paulo Carneiro Aramuni
ORCID: https://orcid.org/0000-0001-7538-5927
Universidade Fumec, Brasil
E-mail: joaopauloaramuni@fumec.br

Resumo

Junto às redes Wi-Fi, em alta na atual era da informação, surgiram também novos riscos aos usuários e às instituições de ensino superior que proveem esse tipo de rede. O objetivo deste trabalho foi analisar, por meio de um Teste de Penetração (Pentest), as vulnerabilidades e ameaças presentes nas redes Wi-Fi de Instituições de Ensino Superior (IES) de Belo Horizonte e de cidades do interior de Minas Gerais próximas da capital. A coleta de dados realizou-se por meio de teste experimental – Pentesting in loco - em redes Wireless Local Area Network (WLAN) das 12 Instituições de Ensino Superior participantes. Os resultados mostraram que a infraestrutura das redes Wi-Fi das IES é muito diversificada e que uma porcentagem

significativa dessas WLAN se encontra vulnerável e pode ser ameaçada por usuários maliciosos.

Palavras-chave: Wi-Fi; Pentest; Análise de Vulnerabilidades.

Abstract

Along with Wi-Fi networks, which are on the rise in today's information age, new risks have also emerged for users and higher education institutions providing such networks. The objective of this study was to analyze, through a Penetration Test (Pentest), the vulnerabilities and threats present in the Wi-Fi networks of Higher Education Institutions (HEIs) of Belo Horizonte and of cities in the interior of Minas Gerais near the capital. . Data collection was performed through experimental testing - Pentesting in loco - in Wireless Local Area Network (WLAN) of the 12 participating Higher Education Institutions. The results showed that IES Wi-Fi network infrastructure is very diverse and that a significant percentage of these WLANs are vulnerable and may be threatened by malicious users.

Keywords: Wi-Fi; Pentest; Vulnerability Analysis.

Resumen

Junto con las redes Wi-Fi, que están en aumento en la era de la información de hoy, también han surgido nuevos riesgos para los usuarios y las instituciones de educación superior que proporcionan dichas redes. El objetivo de este estudio fue analizar, a través de una Prueba de penetración (Pentest), las vulnerabilidades y amenazas presentes en las redes Wi-Fi de las instituciones de educación superior (IES) de Belo Horizonte y las ciudades del interior de Minas Gerais, cerca de la capital. . La recolección de datos se realizó a través de pruebas experimentales (Pentesting in loco) en la Red de área local inalámbrica (WLAN) de las 12 instituciones de educación superior participantes. Los resultados mostraron que la infraestructura de red Wi-Fi de IES es muy diversa y que un porcentaje significativo de estas WLAN son vulnerables y pueden estar amenazadas por usuarios malintencionados.

Palabras clave: Wi-Fi; Pentest; Análisis de vulnerabilidad.

1. Introdução

As redes Wi-Fi trouxeram uma grande praticidade para vida das pessoas, proporcionando grande liberdade no acesso, baixo custo de implementação, facilidade de instalação e configuração (Ramachandran, 2011; Rufino, 2014). Entretanto, novos riscos

surgiram com a adoção crescente e maciça dessa nova tecnologia. A frequência de tentativas de violação e ataques a essas redes tem se intensificado nos últimos anos (Ramachandran, 2011). Administradores sem muito conhecimento ou com desejo impulsivo de aderência rápida a essas novas demandas deixam de lado as práticas de gestão e segurança das redes Wi-Fi (Ramachandran, 2011; Rufino, 2014).

Vasconcellos (2013) afirma que um problema importante na segurança das redes Wi-Fi está fortemente ligado ao desconhecimento e despreparo dos administradores e usuários na implementação e uso dos recursos de segurança disponíveis.

Pesquisa divulgada pela Internet Census, publicada por Botnet (2012), mostrou que a ativação de dispositivos Wi-Fi em redes com as configurações-padrão de fábrica como, por exemplo, usuários e senhas já pré-configurandas pelos fornecedores, é muito comum. Segundo essa pesquisa, cerca de 1,2 milhões de dispositivos foram analisados e, desses, 420 mil dispositivos estão sujeitos à exploração e invasão devido ao uso de configurações-padrão disponibilizadas pelos fabricantes em manuais em sites.

As instituições de ensino, visando atender às necessidades de seus alunos, professores e colaboradores, têm disponibilizado redes Wi-Fi para a comunidade acadêmica. Essas redes têm um uso bem diversificado. Nelas são acessados sistemas WEB acadêmicos da própria instituição, aplicativos de acesso informações institucionais (notas, presenças, e-mails), redes sociais, aplicativos de comunicação e Internet de forma geral.

Diante desse contexto, apresenta-se o problema norteador da pesquisa: no âmbito da segurança da informação, quais são as principais vulnerabilidades e ameaças presentes em redes Wi-Fi de grandes instituições de ensino superior de Belo Horizonte (Minas Gerais) e de cidades próximas da capital?

Desta forma, o objetivo deste artigo foi analisar a presença de vulnerabilidades e de ameaças que coloca em risco a segurança da informação em redes IEEE 802.11 (Wi-Fi) de grandes Instituições de Ensino Superior de Belo Horizonte (Minas Gerais) e de cidades próximas da capital.

Este trabalho se justifica em função de que nas redes Wi-Fi de Instituições de Ensino Superior, a demanda pelo tráfego de dados e disponibilidade desses serviços é muito significativa. Essas redes transportam informações sensíveis à comunidade acadêmica e as de seus sistemas e, também, os dados privados e sigilosos de seus utilizadores, sendo de vital importância resguardar e manter esses ativos seguros. Para se alcançar essas garantias, é necessário aprofundar os conhecimentos das principais vulnerabilidades e ameaças presentes nesse tipo de ambiente de rede, bem como buscar alternativas de controles de segurança que

possam mitigar os riscos que essas redes Wi-Fi trouxeram aos ambientes acadêmicos e a seus usuários.

A presente pesquisa baseou-se na metodologia de teste de penetração da OSSTMM-3 e buscou avaliar os itens confidencialidade, integridade, disponibilidade, autenticação e controle de acesso das redes WLAN. Além disso, a pesquisa adotou as etapas do Pentest propostas na metodologia de Ramachardran & Buchanan (2015), divididas em Planning, Discovery, Attack e Report.

2 - Revisão da Literatura

2.1 Redes WLAN (Wireless Local Area Network) e o Padrão IEEE 802.11

Em meados dos anos 80, a Federal Communications Commission (FCC), órgão regulador norte-americano para telecomunicações e radiodifusão, desvencilhou parte dos espectros de frequência para desenvolvimento livre, sem a necessidade de licenciamento e de pagamento para utilização de determinadas faixas de frequência. As faixas de frequência dedicadas para Industrial Scientific and Medical (ISM) são bandas reservadas internacionalmente para o desenvolvimento Industrial, científico e médico. Para isso, foram criadas normas de limitação de potência de transmissão e técnicas de modulação dentro dessas faixas.

Este padrão foi internacionalmente difundido e adotado em diversos países e, também, no Brasil, com algumas ressalvas. No Brasil, a legislação para esse tipo de sistema foi inicialmente definida pela ANATEL, por meio da Norma 02/93, posteriormente pela Norma 012/96 (resolução 209 de jan/2000), e atualmente, pela resolução 506 de jul/2008 – Regulamento sobre Equipamentos de Radiocomunicação de Radiação Restrita.

Conforme destaca Gast (2005), o padrão IEEE 802.11 tem recebido diferentes designações. O padrão é chamado de Ethernet sem fio em referência ao padrão de redes cabeadas IEEE 802.3. O nome Wi-Fi é definido pela organização Wi-Fi Alliance a partir do programa de certificação de interoperabilidade de produtos que utilizam o padrão IEEE 802.11. As redes sem fio 802.11 também são chamadas de redes locais sem fio ou WLAN (Wireless Local Area Network), em referência à topologia de redes locais LAN (Local Area Network).

O IEEE desenvolveu diversos padrões e subpadrões para tecnologia de WLAN, entre eles, destacam-se os subpadrões 802.11a, 802.11b, 802.11g, 802.11n e 802.11ac. Esses padrões

diferem em relação à frequência de operação, taxa de transmissão, largura de banda, à modulação utilizada para transmissão dos dados e recursos de segurança suportados.

O IEEE evoluiu as capacidades do padrão 802.11 original e, em 1999, foi criada a especificação 802.11b. Este padrão suporta taxa máxima de transmissão de até 11 Mbps, utilizando a mesma frequência de rádio regulamentada de 2,4 GHz do padrão 802.11 original. É mais vulnerável a interferências de outros dispositivos de mesma frequência como telefones sem fio e forno micro-ondas (Caçador, 2014; Gast, 2005).

Em paralelo ao desenvolvimento 802.11b, o IEEE criou uma segunda extensão para o padrão 802.11 definido como 802.11a, que suporta velocidade de transmissão de até 54 Mbps e sinais em um espectro de frequência regulamentado na faixa de 5 GHz. Como as redes 802.11b e 802.11 utilizam frequências diferentes, as duas tecnologias são incompatíveis. As maiores vantagens do padrão 802.11a em relação ao 802.11b são suas maiores taxas de transmissão 54Mbps e menor interferência de outros dispositivos como telefones sem fio e forno micro-ondas (Scarfone et al., 2008).

O termo vulnerabilidade para segurança da informação é tratado como um ponto fraco, um erro (bug), ou seja, uma deficiência ou falha que pode ser explorada em um determinado software/hardware, protocolo, ferramenta, algoritmo, equipamento ou processo.

Os recursos criptográficos e os processos de autenticação e controle de acesso são de vital importância para as WLAN. Seu uso é sempre recomentado, porém nem sempre são imunes a falhas ou a quebras. O conhecimento desses mecanismos de criptografia, autenticação e verificação de integridade foi fundamental para a concepção e realização da etapa experimental da presente pesquisa.

Waliullah & Gan (2014) e Welch & Lathrop (2003) classificam os ataques em dois tipos: ataques passivos e ataques ativos. Nos ataques passivos, um atacante tenta obter informações da rede apenas observando/coletando o trafego que passa pela WLAN. Nesse tipo, o invasor não produz nem modifica dado da rede. Os dois tipos mais comuns são: Análise de Trafego (Traffic Analysis); Espionagem (Eavesdropping). Já nos ataques ativos, o invasor escuta, gera e modifica informações/dados da rede atacada. Uma quantidade maior de ataques se enquadra nessa classificação como: Negação de Serviço (Denial of Service); Injeção de Pacote (Replay Attack); Sequestro de Sessão (Session Highjacking); Pontos de Acesso Maliciosos (Rogue Access Point); Intermediação de conexão (Main in the Middle); Acesso não Autorizado (Unauthorized Access).

2.2 -Teste de penetração (Pentesting)

Para Bacudio et al. (2011), os testes de penetração ou pentesting são um conjunto de atividades realizadas para identificar e explorar falhas e vulnerabilidades de segurança. Ele ajuda a medir o nível de robustez e a segurança que foram implementadas. A metodologia do teste de penetração, inclui três fases: preparação da avaliação, testes e análise de teste. A fase de teste envolve as seguintes etapas: coleta de informações, análise de vulnerabilidade e exploração de vulnerabilidade.

Direcionados exclusivamente a Pentesting em redes padrão 802.11, o trabalho de Ramachandran & Buchanan (2015) e Ramachandran (2011) divide os testes de penetração em quatro etapas: Planning, Discovery, Attack e Report. As etapas (fases) apresentadas pelos autores supracitados serviram de base para a definição das fases do experimento da presente pesquisa.

Para um processo de levantamento desses riscos e também no intuito de criar um guia para melhoria de segurança nessas redes, as técnicas de teste de penetração são um processo eficiente e muito utilizado em redes que já estejam em produção ou queiram passar por uma avaliação/auditora (Weidman, 2014).

Em relação à estratégia do teste de penetração, pode-se separá-los em três estratégias: Teste Caixa Preta (Black Box), Teste Caixa Branca (White Box) e Teste Caixa Cinza (Grey Box). Todas as três estratégias estão relacionadas à quantidade de informações previas recebidas pelo pentester (Shravan, Neha e Pawan, 2014).

No teste Caixa Preta, o avaliador não recebe qualquer tipo de informação sobre o ambiente a ser analisado. O intuído é colocar o pentester em condições reais, em que um atacante externo, que não tem conhecimento algum de sua rede, irá buscar uma forma de invasão. No teste Caixa Branca, o avaliador recebe uma grande quantidade de informações sobre o ambiente a ser analisado. Nessa estratégia, o foco é simular um ataque interno, em que o atacante tem conhecimento sobre a rede, sistemas e pessoas. No teste Caixa Cinza, o avaliador recebe certo nível de informação sobre o ambiente, informações que possivelmente são públicas ou fáceis de conseguir.

3 – Metodologia da Pesquisa

Considerando o direcionamento proposto para este estudo, que visa identificar as estratégias e técnicas para quebrar a segurança da informação em instituições de ensino, a pesquisa classifica-se, quanto aos objetivos, como exploratória. De acordo com Pereira (2018),

nos estudos exploratórios, analíticos ou descritivos, uma forma de investigação muito utilizada é o Estudo de Caso (EC). Um caso é um acontecimento ou um fenômeno em estudo. O EC é uma metodologia de estudo de fenômenos individuais ou, processos sociais.

Em relação à abordagem do problema, a pesquisa caracteriza-se como qualitativa. Ainda segundo Pereira (2018), os métodos qualitativos são aqueles nos quais é importante a interpretação por parte do pesquisador com suas opiniões sobre o fenômeno em estudo. Neles a coleta de dados muitas vezes ocorre por meio de entrevistas com questões abertas. Neste tipo de pesquisa algumas características, conforme Ludke e Andre (2013), são:

1) A pesquisa qualitativa, em geral, ocorre no ambiente natural com coleta direta de dados e o pesquisador é o principal instrumento;

2) Os dados coletados são preferencialmente descritivos;

3) A preocupação do processo é predominante em relação à do produto;

4) O "significado" que as pessoas dão as coisas e a sua vida são focos de atenção para o pesquisador e,

5) A análise de dados e informações tende a seguir um processo indutivo.

Todas as instituições estudadas enquadram-se como Instituição de Ensino Superior (IES), em sua grande maioria, 75%, em Belo Horizonte e algumas, 25%, no interior de Minas Gerais. Doze instituições aceitaram participar da pesquisa, conforme Tabela 1.

Tabela 1 - Classificação das EIS participantes do experimento.

Instituição	Alunos	Campus	Cursos
A	13.000	4	45
B	1.800	2	4
C	19.000	5	55
D	16.000	2	52
E	33.000	3	99
F	1.300	1	5
G	18.000	3	38
H	8.000	2	21
I	23.000	13	52
J	1.500	2	22
K	49.000	8	120
L	4.000	1	4

Fonte – Dados da pesquisa, 2019.

A Tabela 1 demonstra alguns dados descritivos sobre as instituições de ensino pesquisadas. O nome das instituições, bem como dos participantes da pesquisa, foram preservados.

A coleta de dados realizou-se por meio de Testes de Penetração (Pentesting) em redes WLAN de Instituições de Ensino Superior. As diretrizes do manual OSSTMM-3 (Open Source Security Testing Methodology Manual) foram escolhidas para realização do Pentesting porque esta é uma importante referência na área de segurança de redes e está em constante atualização (Allen, Heriyanto e Ali, 2014; Scarfone, Orebaugh, 2008)

No intuito de facilitar as etapas de coleta de dados, os autores optaram por utilizar o Sistema Operacional Kali Linux versão 2016.1. Trata-se de uma distribuição Linux desenvolvida para auditoria e teste de penetração em sistemas, redes, aplicativos, banco de dados e demais ambientes computacionais. O Kali Linux apresenta, em sua estrutura, uma suíte de ferramentas destinadas à análise do padrão 802.11. (Ramachandran e Buchana, 2015; Beggs, 2014; Allen, Heriyanto e Ali, 2014).

Para Pentest em WLAN, esse sistema operacional disponibiliza em torno de trinta ferramentas com propostas de avaliações para diversos tipos de vulnerabilidades.

No experimento de campo realizado, o processo do Pentest foi dividido em quatro etapas: planejamento (escopo), descobertas, vulnerabilidades e exploração. No planejamento, os procedimentos dos testes de invasão foram feitos nos espaços de convivência ou áreas de grande concentração de pessoas nas instituições escolhidas, com o objetivo de observar e analisar a segurança dos pontos de acesso (Access Point AP) e estações (STAs)/usuários dessas WLAN. Na fase de descoberta, o procedimento experimental foi feita in loco e o objetivo principal dessa fase foi levantar informações referentes ao ambiente da rede sem fio. A grande maioria dos autores pesquisados, como Waliullah, Moniruzzman e Rahman (2015), Frankel et al. (2007) e Welch e Lathrop (2003), considera essa etapa como uma análise de tráfego (Traffic Analysis). Nesta pesquisa, utilizou-se ferramentas de análise passiva (não gera interferência no funcionamento e fluxo da rede) de rede para enumerar e obter informações relativas ao/s Access Points (AP) e clientes (STA) dessas redes. Na fase de vulnerabildiades, os ataques foram classificados em categorias seguindo os critérios de Waliullah e Gan (2014), Sobh (2013) e Phifer (2011) que são: ataques contra a autenticação, confidencialidade, integridade, disponibilidade, controle de acesso. E na última etapa, exploração, mediante levantamento das informações coletadas na etapa de descoberta e vulnerabilidades a elas associadas, o procedimento experimental seguiu a fase de exploração (ataques) de falhas das WLAN.

As informações coletadas nas redes avaliadas na etapa experimental (teste de penetração) foram analisadas de forma qualitativa. As vulnerabilidades testadas e encontradas nos ambientes avaliados foram classificadas em relação à confidencialidade, integridade, disponibilidade, autenticação ou aos controles de acesso (Phifer, 2011; Sobh, 2013; Waliullah e Gan, 2014). Também foi feita uma comparação mostrando quais os controles de segurança sugeridos na ISO/IEC 27002:2013 não estavam sendo cobertos pelas redes testadas em relação as suas vulnerabilidades estabelecidas pela ABNT (2013).

4. Análise e discussão dos resultados

O Quadro 1 apresenta uma síntese das possíveis perdas de confidencialidade, integridade, disponibilidade, autenticação e controle de acesso observados na coleta de dados nas instituições participantes da pesquisa. Além disso, descreve as ausências dos controles propostos pela ISO 27002, os ataques aplicados nos testes e também os possíveis ataques descritos na literatura.

Quadro 1: Síntese dos Resultados.

IES	Perda da Confidencialidade	Perda da Integridade	Perda da Disponibilidade	Perda da Autenticação	Perda da Controle de Acesso	Controles ISO 27002 não aplicados	Ataques possíveis e bem-sucedidos
A e F	- Não há implementação de protocolos para criptografia de dados a nível de camada 2 padrão 802.11 - Dados trafegando em texto claro - Possível atuação de elementos maliciosos na WLAN. (APs falsos)	- Pacotes podem ser forjados e enviados as STAs	- Não há proteção dos quadros (*frames*) de controle e gerenciamento. - Canais sobrepostos e conflitantes	- Não há implementado de mecanismo de autenticação	- Controle de Acesso feito pelo End. MAC das STAs	- Política de controle de acesso - Acesso às redes e aos serviços de rede - Restrições de acesso à informação - Controles Criptográficos - Controles de Redes - Segurança dos serviços de rede - Proteção e privacidade de informações de identificação pessoal	- *Eavesdropping* - *Man in the Middle* - *Evil Twin AP* - *Rogue AP* - *Replay Attack* - *Frame Injection Attack* - *Dos Attack* - *MAC Address Sppofing* - *Unauthorized Access* - *Network Scanning*
B	- Possível atuação de elementos maliciosos na WLAN. (APs falsos)	- Pacotes podem ser forjados e enviados por STAs autenticadas participantes da rede	- Não há proteção dos quadros (*frames*) de controle e gerenciamento	- Mecanismo de autenticação em nível *Personal e passphrase* fraca e de fácil dedução	- Controle de acesso parcial da rede. - Implementação de *Hotspot* para acesso a Internet	- Acesso às redes e aos serviços de rede - Controles de Redes - Segurança dos serviços de rede	- *ARP Spoofing* - *HotSpot Spoofing* - *Unauthorized Access* - *Network Scanning* - *Rogue AP*
	- Não há implementação de protocolos para criptografia de dados a nível de camada 2 padrão 802.11 em uma das ESSs	-Pacotes podem ser forjados e enviados por STAs autenticadas ou não autenticadas na rede	- Não há proteção dos quadros (*frames*) de controle e gerenciamento	- Não há implementado de mecanismo de autenticação - Mecanismo de autenticação em nível *Personal e passphrase* fraca e de fácil dedução.	- Controle de acesso parcial da rede - Implementação de *Hotspot* para acesso a Internet	- Acesso às redes e aos serviços de rede - Controles de Redes - Segurança dos serviços de rede	- *Eavesdropping* - *Man in the Middle* - *Evil Twin AP* - *Rogue AP* - *HotSpot Spoofing* - *Replay Attack*

C, I e H	- Dados trafegando em texto claro - Possível atuação de elementos maliciosos na WLAN. (APs falsos)			- Certificado Auto Assinado		- Proteção e privacidade de informações de identificação pessoal	- *Frame Injection Attack* - *Dos Attack* - *802.1X Identity Theft* - *Unauthorized Access* - *Network Scanning*
D e E	- Possível atuação de elementos maliciosos na WLAN. (APs falsos)	- Pacotes podem ser forjados e enviados por STAs autenticadas participantes da rede	- Não há proteção dos quadros (*frames*) de controle e gerenciamento.	- Mecanismo de autenticação *Enterprise* robusto mas com possibilidade de roubo de credencias de acesso	- Garantia atrelada a robustez da senha dos usuários	- Proteção e privacidade de informações de identificação pessoal	- *Evil Twin AP* - *Rogue AP* - *Replay Attack* - *Dos Attack* - *802.1X Identity Theft*
G	- Não há implementação de protocolos para criptografia de dados a nível de camada 2 padrão 802.11 - Dados trafegando em texto claro - Possível atuação de elementos maliciosos na WLAN. (APs falsos)	- Pacotes podem ser forjados e enviados as STAs	- Não há proteção dos quadros (*frames*) de controle e gerenciamento - Canais sobrepostos e conflitantes	- Não há implementado de mecanismo de autenticação	- Controle de acesso parcial da rede - Implementação de *Hotspot* para acesso a Internet	- Política de controle de acesso - Acesso às redes e aos serviços de rede - Restrições de acesso à informação - Controles Criptográficos - Controles de Redes - Segurança dos serviços de rede	- *Eavesdropping* - *Man in the Middle* - *Evil Twin AP* - *Rogue AP* - *Replay Attack* - *Frame Injection Attack* - *Dos Attack* - *Unauthorized Access* - *Network Scanning*
J	- Não há implementação de protocolos para criptografia de dados a nível de camada 2 padrão 802.11 - Dados trafegando em texto claro - Possível atuação de elementos maliciosos na WLAN. (APs falsos)	-Pacotes podem ser forjados e enviados as STAs	- Não há proteção dos quadros (*frames*) de controle e gerenciamento Canais sobrepostos e conflitantes	- Não há implementado de mecanismo de autenticação - Mecanismo de autenticação em nível *Personal e passphrase* fraca e de fácil dedução	- Controle de Acesso feito pelo End. MAC das STAs	- Política de controle de acesso - Acesso às redes e aos serviços de rede - Restrições de acesso à informação - Controles Criptográficos - Controles de Redes - Segurança dos serviços de rede - Proteção e privacidade de informações de identificação pessoal	- *Eavesdropping* - *Man in the Middle* - *Evil Twin AP* - *Rogue AP* - *Replay Attack* - *Frame Injection Attack* - *Dos Attack* - *MAC Address Sppofing* - *Unauthorized Access* - *Network Scanning-*
K	- Possível atuação de elementos maliciosos na WLAN. (APs falsos)	- Pacotes podem ser forjados e enviados por STAs autenticadas participantes da rede	- Não há proteção dos quadros (*frames*) de controle e gerenciamento.	-Mecanismo de autenticação em nível *Personal e passphrase* fraca e de fácil dedução. - Mecanismo de autenticação *Enterprise* robusto mas com possibilidade de roubo de credencias de acesso	- Controle de acesso parcial da rede. - Implementação de *Hotspot* para acesso a Internet. - Garantia atrelada a robustez da senha dos usuários para a rede *Enterprise*	- Acesso às redes e aos serviços de rede - Proteção e privacidade de informações de identificação pessoal	- *Evil Twin AP* - *Rogue AP* - *HotSpot Spoofing* - *Dos Attack* - *802.1X Identity Theft* - *Unauthorized Access*
L	- Possível atuação de elementos maliciosos na WLAN. (APs falsos)	- Pacotes podem ser forjados e enviados por STAs autenticadas participantes da rede	- Não há proteção dos quadros (*frames*) de controle e gerenciamento.	- Mecanismo de autenticação em nível *Personal e passphrase* fraca e de fácil dedução	- Controle de acesso parcial da rede	- Acesso às redes e aos serviços de rede - Controles de Redes - Segurança dos serviços de rede	- *ARP Spoofing* - *Unauthorized Access* - *Network Scanning* - *Rogue AP*

Fonte: Dados da Pesquisa, 2019.

O quadro 1 expõe de maneira objetiva os ataques possíveis e bem-sucedidos dentro das instituições de ensino pesquisadas. Tratam-se de dados preocupantes que devem ser levados em consideração para garantir a segurança da informação e prevenir fraudes contra estudantes, professores e funcionários que compõem a instituição.

Após a coleta de dados do experimento, pode-se observar uma expressiva utilização do modelo de rede Wi-Fi em modo Personal (WPA2-PSK). Esse padrão é indicado para redes de pequeno porte e com pequena quantidade de usuários e STAs. Sendo assim, das 12 Instituições analisadas, somente duas, ou seja, 16% implementaram integralmente em sua infraestrutura WLAN o modo Enterprise, indicado para redes Wi-Fi de grande porte e com número elevado de utilizadores e dispositivos.

No modo Personal, a utilização de uma passphrase é obrigatoria para a autenticação na rede. O grande problema dessa solução para redes com muitos usuários e dispositivos, como o observado nas IES, é a qualidade e o sigilo dessa passphrase (senha). Das 10 instituições que não adotaram padrão Enterprise, em 60% delas a senha era muito fraca (sucesso em ataques de dicionário ou de força bruta) ou publicamente divulgada.

Um dado muito importante coletado pelo experimento e que expõe gravemente os utilizadores dessas redes é o modo de operação Open. Nesse modo, nenhuma criptografia é aplicada em nível de camada 2, sendo possível capturar, visualizar ou manipular (criar, modificar, direcionar, bloquear) todo o tráfego dos usuários participantes. Das 12 IES participantes, sete delas, ou seja, 58% tinham alguma infraestrutura atuando em modo Open. Esse dado é muito relevante e de grande preocupação.

Uma constatação também observada na análise foi a utilização significativa de mecanismos de autenticação Hotspot para o acesso à Internet dessas Instituições. Metade das redes estudadas dispunham de algum mecanismo Hotspot para validação e liberação de acesso à Internet. E em um total de seis redes, apenas uma utilizava o protocolo HTTPS para acesso à página de login do portal HotSpot. Todos os HotSpots tiveram suas páginas de autenticação capturadas e clonadas facilmente para o roubo das credências dos usuários.

Dois pontos observados em todas as redes estudadas foi a presença de diderentes ESSIDs no raio de cobertura das instituições e que, em sua maioria, eram desconhecidos pelos administradores. Esses SSIDs podem caracterizar-se como Rogue APs ligados ao ambiente de rede. E o segundo ponto é referente à ausência de proteção dos Frames de controle, o que possibilita facilmente os ataques de negação de serviço (DoS).

5 – Considerações Finais

Como o processo de crescimento e utilização das tecnologias de informação e comunicação é muito acelerado, a segurança da informação deve ser um ponto de preocupação e atenção na adoção de redes Wi-Fi em IES. Buscou-se, portanto, no objetivo desta pesquisa analisar as vulnerabilidades e ameaças dessas redes padrão IEEE 802.11 em grandes instituições de ensino superior de Belo Horizontes (MG) e de cidades próximas da capital.

Pôde-se observar que todas as WLAN das IES analisadas apresentaram algum tipo de vulnerabilidade e demonstraram nível de segurança ainda deficitário. Além disso, observaram-se também algumas falhas primárias, dentre elas, a ausência de criptografia, utilização de padrão de redes de pequeno porte (modo Personal), senhas de conhecimento público ou de fácil dedução, sistemas Hotspot com conexões sem criptografia e ausência de ferramentas de detecção de APs falsos. Pontos esses que merecem a atenção outras instituição de ensino pois podem contribuir para a melhoria da segurança das infraestruturas das suas redes Wi-Fi.

Verificou-se no experimento que as redes testadas não cumprem as recomendações técnicas de segurança referentes às questões de confidencialidade, intergridade, disponibilidade, controle de acesso e autenticação dos utilizadores. Em relação à infraestrutura, poucas instituições operavam suas resdes Wi-Fi em modo Enterprise que é a mais indicada e coerente.

As redes WLAN das instituições avaliadas poderiam se tornar mais seguras por meio de pequenas mudanças de baixo investimento. Essas melhorias podem ser alcançadas através da implementação e configuração do modo Enterprise nos Access Point e da configuração de um servidor RADIUS baseado em software livre e para servidor de autenticação. A utilização de certificado digital autoassinado também se mostra bem viável e sem custos financeiros significativos para sua utilização. Essas medidas proporcionariam aos usuários maiores garantias e proteção dos ativos de informação das instituições e seus usuários.

Como sugestão para trabalhos futuros, pode-se apontar a necessidade de identificação de vulnerabilidades em redes Wi-fi para protocolo 802.11x. São oportunidades para avanços aos quais os pesquisadores e profissionais podem se dedicar.

Referências

Associação Brasileira de normas técnicas. (2013). *ABNT ISO/IEC Guia73:2013. Gestão de Riscos. Vocabulário. Recomendações para uso em normas*. Associação Brasileira de normas técnicas. Rio de Janeiro.

Allen, L., Heriyanto, T. & Ali, S. (2014). Kali Linux: assuring security by penetration testing. [s v.l: s.n.]. Packt Publishing Ltd, 7 de abr. de 2014 - 450 p.

Bacudio, A. G. et al. (2011). An Overview of Penetration Testing. *International Journal of Network Security & Its Applications*, 3(6): 19–38.

Beggs, R. W. (2014). *Mastering Kali Linux for advanced penetration testing*. Fist ed. Birmingham: [s.e.].

Botnet, C. (2012). *Port scanning /0 using insecure embedded devices*. Internet Census. Disponível em: <http://census2012.sourceforge.net/paper.html>. Acesso em: 01 nov. 2019.

Caçador, D. M. (2014). *Segurança e Mobilidade em Redes IEEE 802.11*: Modelo de suporte à decisão na escolha de arquitecturas e tecnologias de redes sem fios. [s.l.] Universidade Católica Portuguesa.

Kang, Y. et al. (2015). Comparative Study of Penetration Test Methods. *Advanced Science and Technology Letters*, 87(1): 34–37.

Lashkari, A. H. et al. (2009). *A Survey on Wireless Security protocols* (WEP , WPA and WPA2 / 802 . 11i). Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on, n. 1 v 3, p. 48–52.

Ludke, M.; Andre, M. E. D. A. *Pesquisa em educação*: uma abordagem qualitativa. 2.ed. São Paulo: EPU, 2013.

Pereira, A.S. et al. (2018). *Metodologia da pesquisa científica*. [*e-book*]. Santa Maria. Ed. UAB/NTE/UFSM. Disponível em: https://repositorio.ufsm.br/bitstream/handle/1/15824/Lic_Computacao_Metodologia-Pesquisa-Cientifica.pdf?sequence=1. Acesso em: 01 nov. 2019.

Philfer, Lisa. (2009). *A list of wireless network attacks*. Disponível em: <http://searchsecurity.techtarget.com/feature> Acesso em: 01 de nov. 2019.

Ramachandran, V. (2011) *BackTrack 5 wireless penetration testing*. 1st ed. Birmingham: [s.e.].

Ramachandran, V.; Buchana, C. (2015). *Kali linux wireless penetration testing beginner ' s guide*. 2nd ed. Birmingham: [s.e.].

Rufino, Nelson Murilo de O. (2014). *Segurança em redes sem fio - Aprenda a proteger suas informações em ambientes Wi-Fi e Bluetooth*. 4. ed. São Paulo: Pearson.

Scarfone, K.; Orebaugh, A. (2008). *Technical Guide to Information Security Testing and Assessment Recommendations of the National Institute of Standards and Technology*. Nist Special Publication, v. 800, p. 1–80.

Shravan, K.; Neha, B.; Pawan, B. (2014). *Penetration testing*: A Review. Compusoft, Faridabad v. 3, n. 4, p. 752–7.

Sobh, S. T. (2013). *Wi-Fi Networks Security and Accessing Control*. International Journal of Computer Network and Information Security, v. 5, n. 7, p. 9–20.

Waliullah, M.; Gan, D. (2014) *Wireless LAN Security Threats & Vulnerabilities*: International Journal of Advanced Computer Science and Applications, v. 5, n. 1, p. 176–183.

Weidman, Georgia. (2014) *Teste de invasão* – Uma introdução prática ao hacking. São Paulo: Novatec.

Welch, D.; Lathrop, S. (2003). *Wireless security threat taxonomy*. Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society, June, p. 76–83.

Porcentagem de contribuição de cada autor no manuscrito

Davis Anderson Figueiredo – 40%

Rodrigo Moreno Marques – 20%

Henrique Cordeiro Martins – 20%

João Paulo Carneiro Aramuni – 20%