revista científica
LINKSCIENCEPLACE
interdisciplinar
Revista Científica Interdisciplinar. ISSN: 2358-8411
Nº 1, volume 2, artigo nº 9, Janeiro/Março 2015
D.O.I: 10.17115/2358-8411/v2n1a9

IMPLEMENTAÇÃO DE SEGURANÇA EM REDES WI-FI COM A UTILIZAÇÃO DE VPN.

IMPLEMENTATION OF SECURITY IN WI-FI NETWORKS WITH THE USE VPN.

Fábio Hugo Souza Matos[1]
Engenheiro Eletricista

Diogo Fontana Ragnini[2]
Engenheiro de Telecomunicações

Paulo de Tarso Carvalho de Oliveira[3]
Engenheiro Eletricista

Fabrício Moraes de Almeida[4]
Doutor em Física

RESUMO

Neste trabalho são tratados os diversos métodos de criptografia existentes para redes Wi-Fi e suas vulnerabilidades, a partir de onde foi realizado um estudo de caso apresentando alguns métodos de quebra das chaves de segurança dessas redes e uma opção de melhoria na segurança do usuário, prevenindo possíveis riscos e ameaças à sua privacidade. As ferramentas que foram utilizadas para a realização do estudo de caso são conhecidas como *aircrack-ng*, *tcpdump, inSSIDer e OpenVPN*, onde todas elas são ferramentas livres, de

[1] Fundação Universidade Federal de Rondônia. E-mail: fabio_hugo08@hotmail.com
[2] Engenharia de telecomunicações (Faculdade Assis Gurgacz). E-mail: diogo.ragnini@oi.net.br
[3] Professor do Departamento de Engenharia Elétrica-Fundação Universidade Federal de Rondônia. E-mail: paulo@unir.br.
[4] Professor / Pesquisador do Programa de Mestrado e Doutorado em Desenvolvimento Regional e Meio Ambiente (PGDRA). Pesquisador do GEITEC/UNIR. Chefe de departamento do curso de bacharelado em Engenharia Elétrica/Fundação Universidade Federal de Rondônia, Brasil. E-mail: dr.fabriciomoraes@gmail.com.

fácil obtenção e de fácil utilização, sem que haja a necessidade de conhecimentos avançados. Em vista do grande crescimento das redes Wi-Fi e do grande aumento de sua utilização, tanto em ambientes residenciais quanto em grandes empresas, a segurança dessas redes chamou muita atenção e se tornou foco de muita preocupação e de muitos estudos. Em uma era em que a informação tem grande valor, é necessário que haja a garantia de que as informações que estão na rede estejam seguras, sem que haja a possibilidade de serem roubadas, alteradas, ou qualquer outra ameaça a sua segurança que possa resultar em algum dano a algo ou alguém. Existem muitas vulnerabilidades nos protocolos de segurança das redes Wi-Fi, já que, por ser uma rede sem fio que tem como meio de transmissão o ar, fica exposto e possui limitações quanto aos métodos de segurança aplicados, por isso a necessidade de implementação de um novo método de segurança. O estudo de caso foi realizado na cidade de Porto Velho/RO(Brasil), onde foram analisadas diversas redes Wi-Fi espalhadas pela cidade para a verificação das seguranças utilizadas e para a exploração das vulnerabilidades das mesmas. Foi possível constatar que a segurança das redes analisadas apresentou fragilidades, deste modo, a proposta de implementação deste trabalho é uma forma de melhorar a segurança das informações que trafegam na rede, garantindo ao usuário a privacidade.

Palavras-chave: Redes de computadores, redes sem fio, Wi-Fi, segurança de rede, vulnerabilidade de redes sem fio, VPN.

ABSTRACT

In this work are mentioned the many existents methods of encryption to Wi-Fi networks and their vulnerabilities, from where a case study were developed presenting some methods of breaking the security keys of these networks and an option for improving the user safety, preventing possible risks and threats to his privacy. The tools that were used for the case study are known as aircrack-ng, tcpdump, inSSIDer and OpenVPN, where all of them are free, easy to obtain and easy to use, without needing any advanced knowledge. Considering the large growth of Wi-Fi networks and the large increase in its use, both in residences and in large enterprises environments, the security of these networks drew much attention and became the focus of much concern and many studies. In an era where information is valuable, there must be a guarantee that the information that are on the network are secured, without the possibility of being stolen, modified, or any other threat to its safety that may result in something or someone damaged. There are many vulnerabilities in the Wi-Fi security protocols, since, being a wireless network that has the air as its transmission medium, it is exposed and has limitations for the matter of the security methods applied, that's why it needs to be implemented with a new security method. The case study was conducted in the city of Porto Velho/RO (Brazil), where many Wi-Fi networks around the city were analyzed to verify which securities were being used and to explore their vulnerabilities. It was possible to see that the security of the analyzed networks were weak, then, the proposed implementation of this work is a way of improving the information security that transits over the network, ensuring user privacy.

Keywords: Computer networks, wireless networks, Wi-Fi, networks security, wireless networks vulnerability, VPN.

1. INTRODUÇÃO

As redes sem fio proporcionam mobilidade, flexibilidade, e muitas outras vantagens em relação às redes com cabeamento, por isso o seu uso se tornou cada vez mais presente no cotidiano das pessoas, estando presentes em diversas áreas, na saúde, na educação, no ambiente empresarial, entre outras. E as redes Wi-Fi, padronizadas pelo IEEE 802.11, passam por crescimento desde a sua criação e proporcionam um padrão de comunicação wireless para os diversos dispositivos. Com o grande aumento de sua utilização, a qualidade da segurança das redes Wi-Fi passou a ser questionada.

A maior das desvantagens das redes sem fio está justamente relacionada ao seu meio de transmissão, o ar. Uma vez que o sinal wireless não é um sinal confinado, fica exposto e pode ser interceptado por qualquer dispositivo capaz de captar sinais sem fio. Deste modo, a segurança dessas redes fica comprometida e se torna motivo de muita preocupação para os seus utilizadores. E uma rede para ser considerada segura tem que oferecer alguns parâmetros, sendo alguns deles: confidencialidade, autenticidade e integridade. Estes e outros serviços são considerados fatores primordiais para garantir segurança às informações que trafegam na rede, sendo indispensáveis para usuários que possuem informações sigilosas na rede.

O objetivo básico da segurança das redes sem fio é impedir os acessos não autorizados e a leitura, alteração ou destruição de qualquer informação contida nessas redes, por isso foram criados protocolos de segurança que seriam capazes de garantir esse objetivo. Porém, esses protocolos possuem vulnerabilidades que podem comprometer toda segurança da rede, que uma vez comprometida, se torna passível a ataques de pessoas mal intencionadas que podem causar dano a algo ou alguém. Além disso, o trabalho tem como intuito apresentar as vulnerabilidades presentes nas redes Wi-Fi, realizando a quebra das chaves de segurança dessas redes utilizando ferramentas livres, e como objetivo específico oferecer uma solução para a privacidade das

informações trafegadas na rede, uma vez que é necessário ter os dados protegidos caso algum invasor consiga obter acesso à rede. Essa solução para a privacidade dar-se-á através da criação de redes privadas virtuais com o software livre *OpenVPN*.

E foram realizados testes na segurança de redes Wi-Fi espalhadas pela cidade de Porto Velho/RO (Brasil), onde foi verificado que a vulnerabilidade dos métodos de criptografia utilizados em redes wireless estava presente em todas as redes analisadas. A partir dessas lacunas foi possível obter o acesso à rede e realizar diversas análises na rede, onde pode ser possível encontrar senhas particulares, fotos pessoais, entre outros.

Por fim, foi feita a implementação da segurança com a utilização de redes privadas virtuais, que têm a função de criar um túnel virtual dentro de redes públicas compartilhadas que garante segurança às informações trafegadas nessas redes. Foi possível então verificar que as informações antes legíveis a qualquer um que invadisse a rede, não estavam mais disponíveis para um intruso. Vale ressaltar que esse método garante uma segurança à informação trafegada, mas também possui vulnerabilidades que podem ser exploradas.

2 METODOLOGIA

A metodologia aplicada neste trabalho compreende uma pesquisa exploratória com abordagem quantitativa, onde será realizada uma pesquisa bibliográfica e um estudo de caso. E a pesquisa exploratória é realizada sobre um problema onde é proporcionada maior familiarização com o mesmo, podendo utilizar um levantamento bibliográfico, e geralmente, assumindo a forma de um estudo de caso com resultados de dados quantitativos ou qualitativos. E tem foco em proporcionar uma visão geral do uso de redes Wi-Fi, concebendo uma maior compreensão e precisão, permitindo uma avaliação de quais conceitos existentes podem ser aplicados ao problema em questão.

Destarte, o processo de pesquisa se realizará por meio da pesquisa bibliográfica, a qual abrange a leitura e interpretação de livros, artigos, documentos, trabalhos acadêmicos, entre outros. A pesquisa bibliográfica é o passo inicial para a construção de um trabalho, de onde é tirada a

fundamentação teórica do estudo. Ela auxilia na definição da justificativa e do problema, assim como na determinação dos objetivos e do produto final do trabalho. E a pesquisa bibliográfica tem como objetivo identificar as diferentes contribuições científicas disponíveis para determinado tema, este trabalho teve como referência bibliográfica de maior relevância os livros: Redes de Computadores, TANENBAUM (2003); Redes Sem Fio, MORAES (2011); Segurança de Redes Sem Fio, RUFINO (2011); e Criptografia e Segurança de Redes, STALLINGS (2012).

E por fim, o estudo de caso pode ser entendido como uma pesquisa específica de um problema, onde é realizado um amplo e detalhado estudo. Neste trabalho será realizado um estudo de caso explicativo na localidade de Porto Velho/RO, onde serão analisadas as redes Wi-Fi, de diversos lugares espalhados pela cidade, por meio de ferramentas livres utilizando o *software* livre Linux – Ubuntu 13.10. As ferramentas utilizadas para as coletas e análises de dados são: *aircrack-ng*, *inSSIDer*, *tcpdump* e *OpenVPN*.

3 REVISÃO DE LITERATURA

Segundo Miranda (2008), as redes de computadores vieram da imprescindibilidade de se compartilhar recursos entre comunidades de usuários geograficamente espalhados. São dadas como um conjunto de computadores e periféricos conectados, localmente e remotamente, com a possibilidade de se comunicarem uns com os outros. E para Alves (1998), a rede de computadores é formada pela interconexão de um conjunto de computadores autônomos, onde não existe relação de mestre/escravo entre eles, o que significa dizer que um não pode controlar o outro. E somente dois computadores já são o suficiente para que seja formada uma rede, não existindo um número máximo predeterminado (MIRANDA, 2008). Dois ou mais computadores devem ser conectados em rede através de algum meio de comunicação (AMORIM, 2011). São utilizados, basicamente, três meios de comunicação: fios ou cabos de cobre, fibras ópticas e transmissão por ondas de rádio (MARX, 2008), conforme Figura 1.

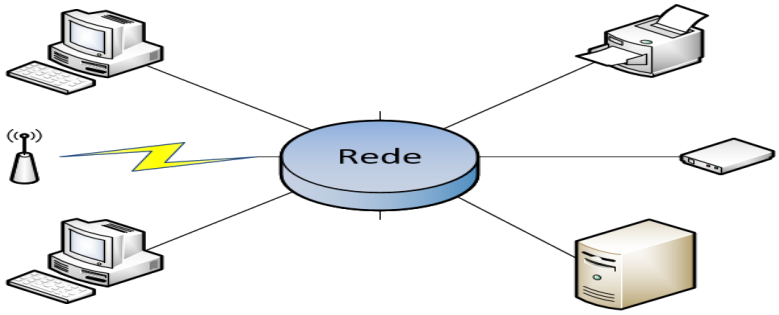

Figura 1: Exemplo de Rede de Computadores. Fonte: Elaboração Própria (VISIO, 2014).

De acordo com Alves (1998), uma rede não precisa ser formada unicamente por computadores, sendo comum a presença de outros dispositivos de rede. Segundo Miranda (2008), as redes de computadores tem como finalidade um meio de comunicação com a disponibilidade de compartilhamento de dados, programas e outros recursos com devida confiabilidade. Com o aumento significativo do conhecimento em redes, foram feitas classificações dividindo-as e fazendo com que a troca de informação entre elas variasse agora de acordo com essa classificação. Foram classificadas de acordo com as tecnologias empregadas, a cobertura geográfica e a velocidade.

Atualmente, há vários tipos específicos, as mais conhecidas são: PAN (*Personal Area Network*), LAN (*Local Area Network*), MAN (*Metropolitan Area Network*) e WAN (*Wide Area Network*) (JARA; AUGUSTO, 2011). (a) PAN (*Personal Area Network*) - Rede de Área Pessoal: A PAN é uma rede doméstica que liga recursos diversos ao longo de uma residência. Um exemplo dela é a tecnologia Bluetooth. A LAN (*Local Area Network*) - Rede de Área Local: são redes de área local ou redes locais, conhecidas também como LANs, são redes de pequena cobertura geográfica que têm como objetivo o compartilhamento de recursos e a troca de informações. São redes privadas utilizando um conjunto de hardware e software que permite conectar computadores individuais e estações de trabalho em escritórios, empresas, escolas, edifícios, contidas numa mesma sala, prédio, ou campus com até alguns quilômetros de extensão. As redes locais tradicionais operam em velocidades entre 10 e 100 Mbps. As mais modernas conseguem atingir

velocidades de até 10 Gbps. Essa rede tem baixo retardo (micro/nano segundos) e são encontradas poucas taxas de erros de transmissão, 10^{-8} a 10^{-11}, (TANENBAUM, 2003).

E MAN (*Metropolitan Area Network*) - Rede de Área Metropolitana: As redes de área metropolitana ou redes metropolitanas, também conhecidas como MANs, são redes que ocupam aproximadamente o espaço de uma cidade e são constituídas de uma ou mais redes LANs, podendo ser uma rede privada ou pública. Por utilizarem tecnologias semelhantes, a rede MAN pode ser entendida como uma versão ampliada de uma LAN, onde os dispositivos em rede podem se comunicar como se fizessem parte de uma mesma rede local. Comparada a LAN, apresenta uma taxa de erro maior, já que possui um maior alcance. São redes comumente encontradas em universidades, hospitais e em organizações com várias delegações espalhadas pela cidade capazes de transportar voz e dados (MIRANDA, 2008). Segundo Tanenbaum (2003), a rede de televisão a cabo é um exemplo de uma rede MAN, a qual abrange mais de uma cidade. Outra MAN surgiu como resultado do desenvolvimento no acesso à Internet sem fio com altas velocidades, padronizada como IEEE 802.16 e denominada de WiMAX.

Para WAN (*Wide Area Network*) - Rede de Área Geograficamente Distribuída: Redes de área geograficamente distribuídas ou redes geograficamente distribuídas, também conhecidas como WANs, são redes de comunicação de dados que abrangem uma grande área geográfica como um país ou um continente. Oferecem transmissão de dados provida por operadoras, como empresas de telefonia e telecomunicações. Devido ao custo elevado na comunicação, essas redes são públicas em sua maioria. A Internet é um exemplo de rede WAN, considerada a maior existente atualmente. Conecta milhões de redes LANs no mundo todo formando uma WAN. Surgiram com a necessidade de ampliação da rede devido ao crescimento das corporações, onde LANs já não eram suficientes para atender a necessidade demandada de informações e recursos compartilhados. Essas redes são formadas por conjuntos de servidores que formam grandes sub-redes que têm como função transportar dados entre os dispositivos de rede, sendo eles

computadores ou outros dispositivos, de um ponto geográfico para outro (MIRANDA, 2008).

Figura 2: Representação das Redes LAN, MAN e WAN. Fonte: Elaboração Própria (VISIO, 2014).

Devido ao crescimento das redes, o compartilhamento de recursos entre os usuários não estava sendo possível. Isso aconteceu com ausência de compatibilidade existente entre as diferentes tecnologias de plataformas de hardware e software das redes que foram criadas, dificultando ou impossibilitando a comunicação entre elas (MIRANDA, 2008). Cada fabricante possuía a sua tecnologia e a mesma só tinha suporte com quem a fabricou, sem a possibilidade de utilizá-la de forma conjunta às diferentes tecnologias. E com o avanço da tecnologia, houve a necessidade de melhorar essa incompatibilidade existente entre as diferentes tecnologias de rede. Assim, teve início uma busca por padrões para que houvesse uma integração entre os produtos dos diferentes fabricantes. E a padronização seria muito bem vinda já que significaria maior lucratividade e mais oportunidades de negócios. Percebendo a importância de tal ação, surgiram organizações para realizar essa padronização, que definiram regras e modelos a serem seguidas pelas empresas para a fabricação de seus produtos (GOMES, 2004).

Além disso, as redes sem fio estão cada vez mais ganhando espaço, estando presentes em ambientes residenciais, empresariais, hospitalares, e

muitos outros. Requerem assim, um alto grau de confiabilidade para os clientes dessas redes, fazendo com que o tema segurança de redes sem fio seja cada vez mais discutido e desenvolvido nessas redes. Então, foram criados protocolos de segurança com o intuito de proteger o acesso de pessoas não autorizadas e proteger os dados trafegados na rede, mantendo assim a autenticidade, a integridade e a confidencialidade da rede.

Segundo Rufino (2011), os métodos de segurança mais utilizados em redes sem fio são: Filtragem do endereço MAC (*Media Access Control*), os protocolos de segurança WEP, WPA (*Wi-Fi Protected Access*) e WPA2. Outro método de segurança que também tem sido bastante utilizado é a VPN (*Virtual Private Network*), que será abordado neste trabalho como a implementação de segurança para garantir a privacidade e a segurança das informações trafegadas em uma rede sem fio. O endereço MAC é um número único presente na interface física dos dispositivos definido pelo seu fabricante e controlado pelo IEEE. Foi criado para permitir a identificação única de um equipamento em relação a qualquer outro endereçamento.

A partir disso, foi criada uma forma de restringir o acesso ao AP de uma rede sem fio aos endereços MAC previamente cadastrado nesse concentrador. E onde somente seria permitida a autenticação de dispositivos possuindo endereços MAC conhecidos e cadastrados pelo AP. O que pode servir como um grande recurso para evitar pessoas não autorizadas de acessarem sua rede, mas que falha na restrição do equipamento, e não do usuário. Isso significa que um usuário que não necessariamente é o portador do equipamento com o endereço MAC cadastrado, pode facilmente, através de técnicas de escuta de tráfego, descobrir um endereço MAC registrado e realizar a clonagem desse endereço, conseguindo assim a autenticação no concentrador. Ainda que possua essa vulnerabilidade, é um método de segurança recomendado e que ajuda na defesa contra acessos não autorizados (RUFINO, 2011).

O protocolo WEP surgiu como uma forma de garantir a segurança das redes sem fio, uma vez que, diferente das redes cabeadas, as redes wireless podem ter seu sinal facilmente interceptado. Portanto, surgiu a necessidade de cifrar os dados trafegados na rede. Esse é o protocolo mais antigo

desenvolvido para garantir a segurança do padrão IEEE 802.11. Esse padrão possui dois modos de autenticação, um chamado de *Open System* e o outro de *Shared Key*. O primeiro modo, como o próprio nome sugere, é um sistema aberto, onde a autenticação é feita sem nenhuma forma de segurança. O segundo modo é baseado em uma chave compartilhada que é realizada na forma *challenge-response*. Uma estação que deseja se conectar a um AP solicita autenticação, então esse concentrador gera e envia um *challenge* para a estação que solicitou a autenticação, onde esse *challenge* é um texto desafio com informações pseudorrandômicas. Após receber o *challenge*, a estação requerente envia para o AP uma *response*, para que a autenticação seja autorizada ou não. A *response* é uma resposta ao AP, contendo as informações recebidas do *challenge* cifradas com o segredo compartilhado. Após o AP receber a *response*, caso a criptografia tenha sido feita com o segredo correto, o acesso é autorizado. A criptografia padrão utilizada nesse modo de chave compartilhada era o WEP. (AMORAS; BRABO; PEREIRA, 2004).

O WEP trabalha com o algoritmo simétrico de criptografia de fluxo denominado de RC4. O RC4 pode possuir 64 *bits* ou 128 *bits*, sendo que, no primeiro caso, 40 *bits* são de chave e os outros 24 *bits* são de um vetor de inicialização (IV – *Initialization Vector*), e, no segundo caso, 104 *bits* são de chave e os outros 24 *bits* são do vetor IV. Utiliza criptografia de chave simétrica, onde existe uma chave secreta para cifrar e decifras os dados trafegados, que deve ser compartilhada entre os dispositivos que querem se conectar a rede e o concentrador.

A chave do protocolo WEP é então composta de uma chave estática e um componente dinâmico (IV), onde esse componente é adicionado à chave para dificultar a descoberta da mesma. É feita então a concatenação desses dois componentes em um primeiro plano. A partir daí é gerado um fluxo de dados pseudorrandômico, que é somado à mensagem a ser transmitida através de uma operação XOR. Finalmente, essa mensagem cifrada é concatenada ao vetor de inicialização e transmitida. O receptor faz o processo reverso para decifrar a mensagem transmitida (MORAES, 2011).

No protocolo WEP, para garantir a integridade de um dado, é realizada a técnica de CRC, a qual gera um ICV (*Integrity Check Value*) para cada dado enviado. Na recepção de um dado, deve-se executar essa técnica CRC e comparar o valor ICV recebido com o gerado, para a verificação da integridade da mensagem, onde caso o ICV seja igual, a mensagem está integra, e caso contrário, sofreu alguma alteração.

Esse protocolo possui algumas vulnerabilidades que fizeram com que novas soluções para a segurança das redes sem fio fossem desenvolvidas. Serão tratadas neste trabalho algumas dessas vulnerabilidades, as quais serão citadas como alguns dos riscos e ameaças à segurança das redes wireless (AMORAS; BRABO; PEREIRA, 2004).

A nova solução para eliminar as vulnerabilidades do protocolo WEP foi o protocolo WPA. Este novo protocolo foi desenvolvido pela Wi-Fi Alliance e lançado um pouco antes do padrão IEEE 802.11i, com a promessa de melhorar os problemas de segurança do antigo protocolo. O protocolo WPA utiliza um novo protocolo para gerenciamento de chaves dinâmicas, o TKIP, que agora gera chaves por pacotes, com o mesmo algoritmo de criptografia utilizado no WEP, o RC4. Porém, o vetor IV antes de 24 *bits* do WEP agora conta com 48 *bits* agregado a novas regras de sequenciamento, o que permite uma melhor e mais segura criptografia dos dados. Também foi inserido o código MIC (*Message Integrity Code*) para realizar as trocas dos números de sequência dos pacotes, melhorando a integridade das mensagens.

O WPA pode funcionar em dois modos, WPA *Personal* e WPA *Enterprise*. No primeiro modo, utiliza uma chave (WPA-PSK (*Pre-Shared Key*)) preestabelecida compartilhada entre o concentrador e as estações que vão se conectar ao mesmo. Foi feito para utilização em pequenas redes. No segundo modo, utiliza o padrão 802.1x para autenticação, que utiliza o protocolo EAP e um servidor RADIUS. Foi feito para utilização em redes de porte maior, empresariais, e necessita de mais um equipamento para a utilização do servidor. O protocolo de segurança WPA também possui vulnerabilidades, as quais serão comentadas como riscos e ameaças à segurança das redes wireless (MORAES, 2011).

O protocolo WPA2 surge então com a homologação do padrão IEEEE 802.11i, sendo baseado nesse padrão e desenvolvido pela Wi-Fi Alliance para aumentar ainda mais a segurança do protocolo WPA no que tange a criptografia e a integridade. Utiliza o protocolo CCMP e não mais o algoritmo RC4, mas sim o algoritmo AES, o qual é considerado mais robusto e faz a criptografia dos dados na forma de blocos ao invés da cifra de byte por byte. Mesmo com o protocolo diferente, foi mantida compatibilidade com o protocolo TKIP e o padrão 802.1x.

Quadro 1: Comparação dos Protocolos WPA x WPA2.

Modo	Tipo	WPA	WPA2
Personal Mode	Autenticação	WPA-PSK	IEEE 802.1X/EAP
	Encriptação	TKIP/MIC	AES
Enterprise Mode	Autenticação	IEEE 802.1X/EAP	IEEE 802.1X/EAP
	Encriptação	TKIP/MIC	AES

Fonte: MORAES (2011).

O WPA2 exige hardwares mais modernos e robustos, já que exige muito mais processamento que os outros protocolos de segurança. O algoritmo AES desse protocolo pode possuir uma chave de até 256 *bits*, que tem um grau de segurança elevado, tornando o padrão WPA2 o padrão atual mais seguro para redes Wi-Fi (MORAES, 2011).

Dessa forma, foi encontrada uma vulnerabilidade nesse protocolo, mas para um usuário já autenticado na rede, onde o mesmo é capaz de realizar a captura dos dados trafegados na rede. Essa vulnerabilidade foi chamada de *Hole 196* (Buraco 196), que tem esse nome pelo fato de ter sido encontrada na página 196 do padrão IEEE 802.11.

3.1 RISCOS E AMEAÇAS À REDE SEM FIO

Manter a segurança de uma rede sem fio tem sido um grande desafio desde o seu surgimento. Como o meio de transmissão é o ar, fica fácil de um sinal wireless ser interceptado, e uma vez interceptado, pode trazer grandes riscos à segurança dessa rede e de grandes consequências.

As redes sem fio são vítimas de muitos ataques realizados de diversas formas, tornando não seguro o tráfego de informações em uma rede wireless, uma vez que quando a rede é vítima de acessos indevidos, se torna sujeita à leitura e alteração dos dados trafegados na rede, o que é uma grande ameaça a quem utiliza essa rede.

Os ataques às redes wireless miram nas fraquezas presentes nas mesmas, nas falhas de segurança que podem apresentar. Essa vulnerabilidade proporciona às pessoas mal intencionadas a invasão e a realização de algum dano a quem utiliza a rede, como roubo de informações, adulteração de dados, e até mesmo, em alguns casos, a destruição de algo que pode comprometer e inutilizar todo um sistema. Tornando assim o utilizador da rede passível de crimes como espionagem industrial, furto em transações bancárias, exposição de informações e conteúdos pessoais (calúnia, difamação e pornografia), entre outros (AGUIAR, 2009).

Assim, fica a necessidade de uma maior garantia na segurança dessas redes por parte dos administradores das mesmas, seja em uma residência ou em uma empresa. É importante também saber que não é uma ferramenta ou tecnologia que protege da melhor forma a rede, devem ser aplicadas mais de uma solução para a melhoria da segurança.

Segundo Rufino (2011), entre os riscos e ameaças à segurança das redes sem fio mais presentes, podem ser citados: segurança física, envio e recepção de sinal, interceptação de sinal, mapeamento do ambiente, captura de tráfego, DoS (*Denial of Service*), configurações de fábrica e vulnerabilidade dos protocolos WEP e WPA. A segurança física está relacionada à segurança quanto à área de abrangência do sinal da rede sem fio, uma vez que o sinal pode alcançar lugares que ultrapassam os limites desejáveis. Sendo assim, é importante ser feito um estudo da área que o sinal pode alcançar que depende do padrão utilizado, da potência de transmissão do AP e também do seu posicionamento (ALBUQUERQUE, 2008). E o posicionamento do AP afeta diretamente na área de envio do sinal, uma vez que ele é o ponto central da transmissão. Assim, é importante posicionar ele de maneira que proporcione um bom desempenho para o cliente levando em conta que a área de abrangência do sinal não deve ultrapassar os limites de utilização do

usuário, para evitar que algum intruso receba o sinal e tente invadir a rede (ALBUQUERQUE, 2008).

Além disso, a interceptação do sinal é um grande problema para as redes sem fio, já que o meio de transmissão não é um meio guiado e pode ser facilmente sintonizado, uma vez que não é possível controlar quem recebe o sinal. Essa interceptação pode ocorrer próximo do aparelho concentrador (AP) ou mesmo realizada a uma grande distância com o uso de equipamentos implementados para melhor captação do sinal do AP. A partir da interceptação, pode ser realizada uma série de ataques à rede (RUFINO, 2011). Já o mapeamento do ambiente é uma ação realizada para identificar as redes sem fio, tentando assim, obter o maior número possível de informações sobre as redes identificadas, para que um ataque seja bem sucedido e para que o intruso não seja detectado. Pode ser considerado o primeiro procedimento para alguém que vai invadir uma rede (ALBUQUERQUE, 2008).

A captura de tráfego se realiza a partir da interceptação do sinal, sem a necessidade de associação à rede, onde, por meio de alguma ferramenta para captura de tráfego, o tráfego de informações de um AP pode ser capturado e copiado. Em uma situação em que não exista segurança nos dados trafegados, é possível obter as informações dos conteúdos trafegados na rede (RUFINO, 2011).

O DoS é uma ameaça que afeta os serviços utilizados na rede, fazendo que eles se tornem indisponíveis. Pode ser feito a partir de um equipamento gerador de frequências na mesma faixa de utilização do AP da rede sem fio, causando assim uma interferência no sinal, ou a partir de uma técnica que sobrecarrega o sistema tornando os recursos indisponíveis para o usuário (RUFINO, 2011).

As configurações de fábrica são um problema que ameaçam a segurança se não forem configuradas pelos administradores da rede. Os equipamentos para as redes wireless vêm de fábrica com mecanismos de seguranças implementados, visto o risco que é uma rede sem segurança, porém eles vêm com configurações padrões, ou seja, podem ser vítimas de ataques facilmente por quem conhece os padrões daquele fabricante (RUFINO, 2011).

O protocolo WEP foi condenado como inseguro após a quebra de seu algoritmo. Ele possui três pontos conhecidos de vulnerabilidade, o compartilhamento de chave, o uso do algoritmo RC4 e o vetor de inicialização (IV). O compartilhamento de chave consiste na distribuição de chaves para os dispositivos que queiram se comunicar, onde os mesmo devem possuir o conhecimento dessa chave. Essa situação se torna inviável em redes de grande porte dada a necessidade de todos os dispositivos conhecerem a chave, o que torna o segredo da chave menos seguro, e dificulta a administração da rede. O algoritmo RC4 ao realizar uma técnica de equivalência numérica, permite que a informação do tamanho da mensagem original seja descoberta, já que a informação gerada no processamento dessa técnica possui o mesmo número de bytes que a original.

O IV utilizado no protocolo WEP tem tamanho de 24 *bits*, que é associado à chave desse padrão, que tem o tamanho padrão de 64 *bits* ou 128 *bits*, onde somente 40 *bits* ou 104 *bits* representam a chave, e os outros 24 *bits* representam o IV. Devido ao tamanho reduzido desse IV, ele se repete várias vezes durante um dia, o que permite a descoberta do IV e a identificação da chave WEP (ALBUQUERQUE, 2008).

O protocolo WPA é considerado mais seguro que o protocolo WEP, já que não tem as mesmas vulnerabilidades. E possui dificuldade maior para ter sua chave quebrada. Mas esse protocolo também tem vulnerabilidades, isto é, está sujeito a ataques de força bruta, onde através de tentativas de diversas senhas, um atacante pode descobrir a chave WPA. No entanto, esses ataques somente são viáveis para chaves com menos de 20 caracteres (RUFINO, 2011).

Outra vulnerabilidade encontrada nesse tipo de protocolo é o ataque de força bruta realizado no WPS (Wi-Fi *Protected Setup*) PIN, que é uma facilidade de configuração para a rede sem fio desenvolvida pela *Wi-Fi Alliance*. Consiste em descobrir o PIN por força bruta, aonde é possível a descoberta da chave WPA. Entretanto, atualmente, muitos fabricantes já desenvolveram métodos para dificultar e até mesmo impossibilitar esse tipo de ataque, que vai desde a desativação dessa configuração WPS, ao desenvolvimento de defesas aos ataques de força bruta. Esse método pode ser

realizado tanto para o protocolo de segurança WPA como para o WPA2 (REAVER SYSTEM, 2014).

Dada as vulnerabilidades das redes sem fio, é preciso no mínimo garantir segurança às informações trafegadas na rede, para que a privacidade e a integridade dos dados sejam mantidas. Neste trabalho será tratada uma forma de prevenir o acesso às informações trafegadas na rede, e acesso ao seu conteúdo, por meio da criação de uma VPN através do software livre OpenVPN.

3.2 IMPLEMENTAÇÃO DE VPN

A VPN é uma rede de comunicação privada virtual, como o próprio nome sugere, criada entre dois pontos, entre redes corporativas e usuários remotos, para que haja segurança na transferência de dados entre esses pontos. Tem algumas das vantagens de um link dedicado e mesma aparência, podendo substituí-lo onde o alto custo para a aplicação do link se torne inviável, porém levando algumas desvantagens, por exemplo, na segurança e no desempenho (CYSCO SYSTEMS, 2004).

Além disso, é uma rede virtual criada no ambiente de uma rede pública, por exemplo, a Internet, com tecnologias de criptografia por tunelamento, onde o tráfego de dados é feito por uma rota dessa rede, criando um túnel privado simulando uma conexão do tipo ponto-a-ponto, com a utilização de protocolos que garantam a confidencialidade, a autenticidade e a integridade dos dados (CYSCO SYSTEMS, 2014). Não são todas as VPNs que são seguras e garantem de fato a privacidade do usuário, existindo assim a necessidade de saber quais os protocolos utilizados pela VPN e saber se a ferramenta a ser utilizada para a sua criação é de confiança.

As VPNs oferecem recursos de autenticação, criptografia e também integridade, sendo uma alternativa econômica e segura para a transmissão de dados entre redes, podendo até tornar seguro o tráfego de informações em redes inseguras. Sistemas de comunicação por VPN têm sido frequentemente encontrados em redes empresarias por sua boa relação de custo/benefício e facilidade de implantação (BORGES; CUNHA; FAGUNDES, 2008).

A autenticação pode ser oferecida por uma verificação de credenciais, *login* e *password*, requisitada para os usuários da rede, para garantir que pessoas não autorizadas não tenham acesso e não possam trocar informações na rede privada. Essa autenticação geralmente é feita a partir de certificados digitais ou chaves públicas. A criptografia é feita para tornar o dado trafegado ilegível para uma situação na qual essa informação seja interceptada em seu trajeto. Para a integridade, é realizada uma autenticação dos dados que verifica a integridade de cada pacote de dados e a origem dos mesmos, caso não seja proveniente de um usuário autorizado (AMORAS; BRABO; PEREIRA, 2004).

Para as redes VPNs podem ser utilizados os protocolos IPSec (IP *Security Protocol*), PPTP (*Point-to-Point Tunneling Protocol*), L2TP (*Layer 2 Tunneling Protocol*), SSL (*Secure Socket Layer*), entre outros (BORGES; CUNHA; FAGUNDES, 2008).

OpenVPN, como o próprio nome diz, é um software livre, Open Source, licenciado pela GPL (*Gerneral Public Licence*), que realiza a criação de VPNs para proporcionar segurança na transmissão de dados via redes públicas. Foi desenvolvido por James Yonan e é disponibilizado para diversos sistemas operacionais, como o Linux, Solaris, Mac OS X, OpenBSD, Microsoft Windows 2000/XP/Vista/7, entre outros.

O software foi baseado no protocolo SSL, implementando soluções de segurança por tunelamento nas camadas OSI 5 ou 6, tendo como ferramenta de recursos de criptografia e autenticação a biblioteca OpenSSL. Permite autenticação por diferentes modos, por credenciais, certificados digitais, chaves secretas compartilhadas, juntamente com suporte a *smart cards*. Consegue transmitir sobre UDP ou TCP, multiplexando toda comunicação em uma única porta TCP/UDP. Estabelece túneis criptografados com a capacidade de estabelecer conexões atrás de NAT (*Network Address Translation*) sem que seja necessária reconfiguração, sendo capaz de criar uma interface virtual para cada VPN baseada na interface genérica TUN/TAP (*Network Tunnel/Tap*), que cria túneis para carregar qualquer tipo de tráfego Ethernet (IP). O OpenVPN não é uma aplicação web e não possui compatibilidade com os protocolos IPSec, L2TP, PPTP. Possui como vantagens a fácil e simples instalação, configuração e utilização, facilidade na depuração de problemas de rede, a

configuração de VPNs para IP fixos e dinâmicos, a compatibilidade com NAT, X.509 PKI, SSL/TLS, certificados RSA, entre outras (OPENVPN TECHNOLIGES, 2014).

Esse protocolo tem como versão mais atual a SSL 3.0 e é tido como antecessor do protocolo TLS (*Transport Layer Security*) padronizado pelo IETF (*Internet Engineering Task Force*), possuem pequenas diferenças, mas que os tornam não interoperacionais. São pronunciados como protocolos semelhantes também denominados de SSL/TLS.

O protocolo SSL utiliza o método de criptografia de chave pública, estabelecendo um canal de comunicação protegido entre o cliente e o servidor, garantindo a segurança e a privacidade dos dados transmitidos na Internet através de autenticação e criptografia (OPPLIGER, 2009). É um método de proteção transparente que estabelece uma sessão segura para os protocolos de aplicação HTTP, POP, SMTP, entre outros. Um exemplo de um servidor web protegido pode ser verificado com a presença do “s” no protocolo de aplicação como em “*https://*”, demonstrando que é certificado pelo protocolo SSL.

O SSL utiliza subprotocolos para estabelecer e iniciar uma conexão segura, podendo ser dividido em *Record Layer Protocol*, *Change Cipher Spec Protocol*, *Alert Protocol*, e *Handshake Protocol*. O *Change Cipher Spec Protocol* é composto de uma mensagem que sinaliza o início de comunicações cliente/servidor seguras e sinaliza possíveis alterações quanto à utilização da criptografia, caso seja necessária sua mudança. O *Alert Protocol* envia mensagens de erros, problemas ou alertas, a respeito da conexão entre cliente e servidor, mensagens estas que especificam o erro ou problema existente e, podem ou não, solicitar ou realizar, a desconexão entre as partes.

O *Handshake Protocol* é responsável pela autenticação cliente/servidor, sendo dividida em duas fases, uma fase para a escolha da chave a ser utilizada entre o cliente e o servidor, para a autenticação do servidor e a troca de chaves pré-mestre, e a outra fase, a qual é optativa, para a autenticação do cliente. No *handshake* é estabelecido uma séria de parâmetros para o protocolo *Record Layer Protocol* e utilizado um código MAC (*Message Authentication Code*) nas trocas de mensagem para maior segurança. E o

funcionamento do *Handshake Protocol* é dividido em nove mensagens, *Client Hello, Server Hello*, *Server Key Exchange*, *Server Hello Done*, *Client Key Exchange*, *Change Cipher Spec*, *Finished*, *Change Cipher Spec* e *Finished* (STALLINGS, 2012).

4. RESULTADOS E DISCUSSÕES

O procedimento inicial para a análise das falhas dos protocolos de segurança das redes Wi-Fi, foi realizado a partir da análise da região, com a ferramenta *inSSIDer*. Primeiramente foi necessário estar com o notebook na interface wireless ativada para executar o *inSSIDer*. Este software é capaz de realizar varreduras no espectro de frequência utilizado pela interface wireless do dispositivo, sendo capaz de gerar gráficos e algumas informações úteis para a análise das redes no alcance da placa wireless. Segue um exemplo de monitoração feita através do *inSSIDer*, conforme Figura 3.

SSID	SIGNAL ▼	CHANNEL	SECURITY	MAC ADDRESS	802.11	VENDOR
Wi-Fi	-35	1	WPA-Personal	5C:D9:98:75:46:D4	g	D-Link Corporation
Milena Reis	-85	11+7	WPA-Personal	00:1A:3F:A9:08:40	n	intelbras
MANTOVANI	-93	6+10	WEP	00:26:5A:1F:7F:36	n	D-Link Corporation
TP-LINK_CA2BEA	-93	6	WPA-Personal	00:27:19:CA:2B:EA	g	TP-LINK TECHNOLOGIES CO.,
WI-FI	-93	11+7	WPA-Personal	00:0A:EB:46:F6:80	n	Shenzhen Tp-Link Technology

Figura 3: Aproximação da Tela de Varredura do InSSIDer. Fonte: Elaboração Própria (2014).

Dentre as informações fornecidas pelo *inSSIDer*, as mais importantes e de maior interesse para a análise neste estudo são: SSID (*Service Set IDentifier*), *Signal* (Nível de Sinal), *Channel* (Canal do AP), *Security* (Protocolo de Segurança), MAC *Address* (Endereço MAC do AP), 802.11 (Padrão WLAN), *Vendor* (Fabricante do AP).

Com essas informações em mãos, já é possível ir para o próximo passo, que é realizar, por meio do software *aircrack-ng*, a quebra das redes que possuem o protocolo WEP. Com essa ferramenta também é possível realizar a análise da região, com a diferença de não tem na informação o tipo de fabricante. A Figura 3, é um exemplo de monitoramento através do *aircrack-ng*, conforme Figura

4.

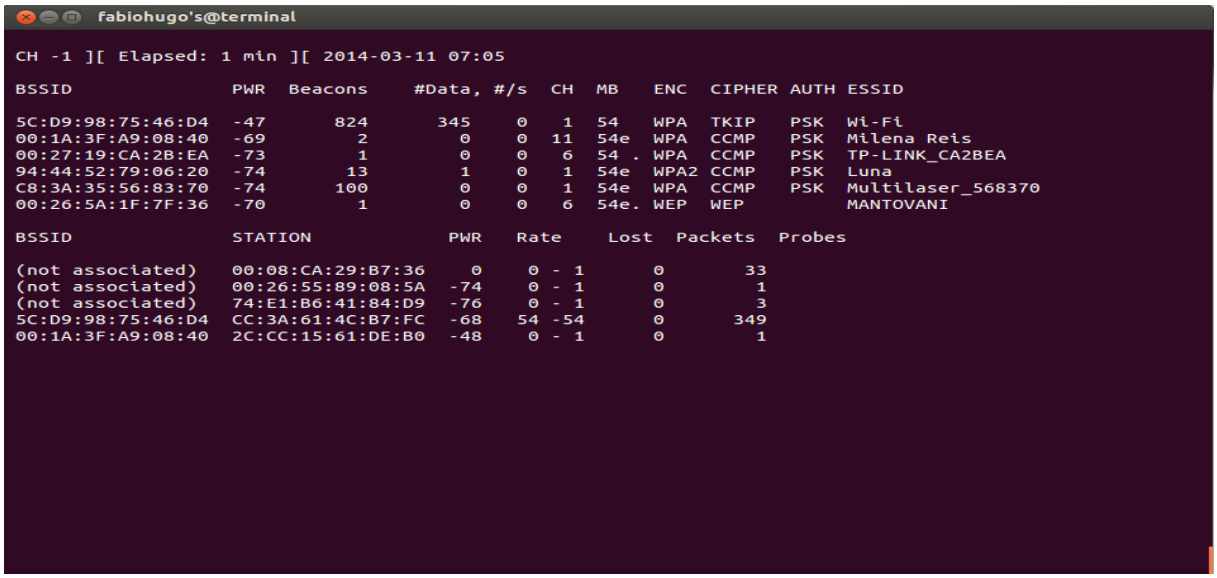

Figura 4: Tela de Captura do Aircrack-ng. Fonte: Elaboração Própria (2014).

O funcionamento do *aircrack-ng* se baseia em dois métodos, um deles parte da captura de pacotes na rede, para poder utilizar esses dados no outro método, o outro realiza ataques estatísticos e de força bruta para tentar descobrir a chave WEP, isso baseado na vulnerabilidade desse protocolo no que relaciona os vetores de inicialização.

O tempo médio para quebrar a senha da criptografia WEP 64 *bits* foi de aproximadamente 15 minutos e o tempo para a criptografia WEP 128 *bits* foi de um pouco mais, 25 minutos. Esse tempo varia de acordo com a dificuldade e tamanho da chave utilizada nas redes, mas que não chega a alcançar muito tempo, dada a facilidade de quebrar a chave de uma criptografia WEP, por ter um tamanho limite de chave pequeno, e pela capacidade do software *aircrack-ng* de fazer os cálculos com velocidade de processamento, alta.

E o procedimento realizado na plataforma Linux com a utilização do *aircrack-ng*: Identificação das redes no alcance da cobertura da placa wireless do notebook utilizado. Para esse procedimento é necessário primeiro que a placa wireless seja coloca em modo promiscuo, ou seja, em um modo de monitoração. Para isso, utiliza-se o comando no terminal do sistema: airmon-ng start (interface de rede padrão wireless – ex: wlan0). Esse modo de monitoramento, também pode ser alcançado realizando os seguintes comandos: ifconfig (interface de rede wireless - ex: wlan0) down; iwconfig

(interface de rede wireless - ex: wlan0) mode monitor; ifconfig (interface de rede wireless - ex: wlan0) up. A partir do momento em que a placa está em modo monitor, a identificação das redes pode ser feita com o comando: airodump-ng (interface de rede wireless modo monitor - ex: wlan0/mon0) e Captura de pacotes.

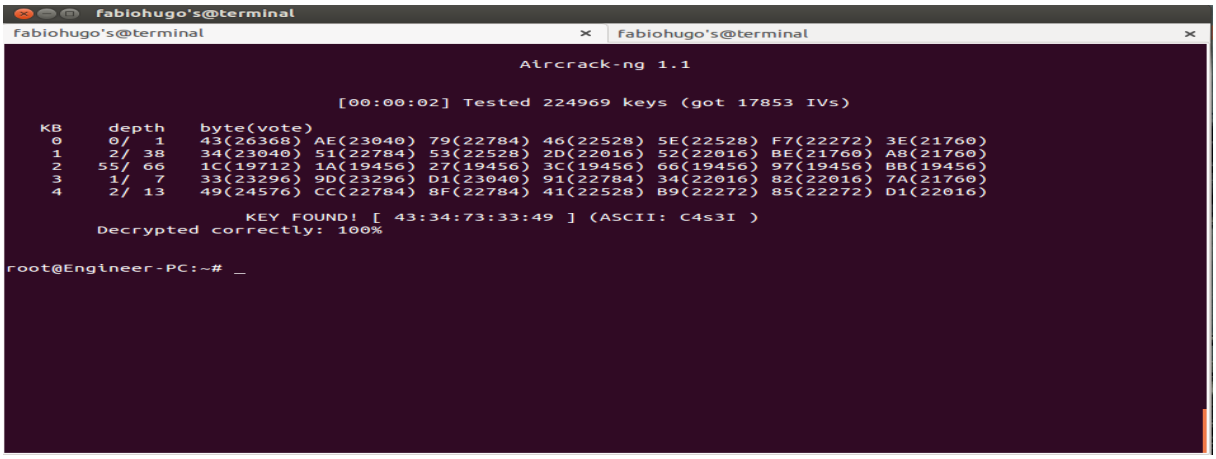

Figura 5: Aircrack-ng Chave WEP 64 Bits. Fonte: Elaboração Própria (2014).

E para realizar a captura dos pacotes é necessária a utilização do comando utilizado para a identificação, mas que agora será configurado para fazer captura de dados: airodump-ng -w (nome do arquivo) --bssid (MAC do AP a ser atacado) --ivs (interface de rede wireless). O w significa *write*, que será o comando para salvar o arquivo de texto; bssid é o endereço MAC do AP monitorado; e ivs indica que serão salvos somente dados dos IVs. O processo de quebra da senha é o último procedimento, onde será utilizado o comando *aircrack-ng* associado ao arquivo salvo na captura de pacotes, para que com os pacotes salvos, o software seja capaz de descobrir a senha WEP, isto é, ircrack-ng (arquivo salvo).ivs. Deste modo, dado o tempo necessário para a captura de pacotes na rede, o *aircrack-ng* será capaz de quebrar a chave. Vale lembrar que o *aircrack-ng* depende da captura de pacotes da rede e que esta depende do tráfego da rede, então o seu tempo varia conforme o grau de utilização da rede. Segue a figura com um exemplo de senha WEP 64 bits quebrada, conforme Figura 5.

As informações que constam na Figura 5, significam: Aircrack-ng 1.1 – Versão utilizado; [00:00:02] – Tempo gasto para quebra da chave; Tested

224969 keys – Número de chaves testadas; (got 17853 IVs) – Número de vetores de inicialização capturados; (KB) – Byte da chave; (depth) –A quantidade de vezes que foram necessários as repetições naquele byte; (byte) – Bytes que vazaram dos IVs; Vote – Votos indicando que o byte está correto; KEY FOUND! – Informação da chave; [43:34:73:33:49] - Informação da chave em hexadecimal; (ASCII: C4s3I) – Informação da chave em ASCII e Decrypted correctly: - Porcentagem de sucesso.

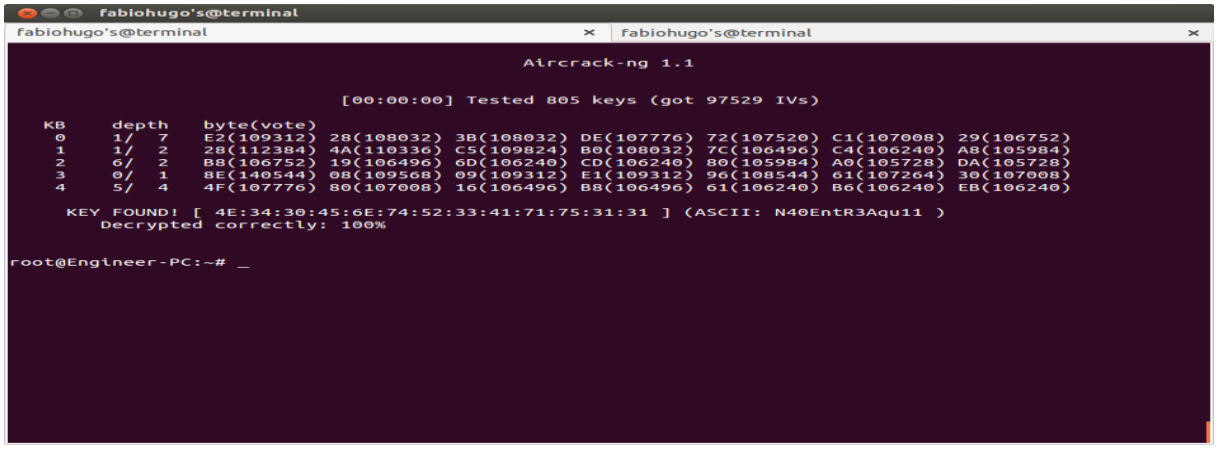

Figura 63: Aircrack-ng Chave WEP 128 Bits. Fonte: Elaboração Própria (2014).

A quantidade de pacotes necessários para a quebra da senha varia de acordo com a dificuldade da mesma. Para o protocolo WEP de 128 *bits* a quantidade de pacotes necessários aumenta bastante. Segue a Figura 6, como exemplo de senha WEP 128 *bits* quebrada. A primeira parte do estudo foi realizada com sucesso, onde foi testada e comprovada a vulnerabilidade dos protocolos WEP. Ao obter acesso nessas redes, foi possível verificar todo o tráfego de dados, concluindo assim que os usuários daquelas redes estão vulneráveis a ataque e que precisam de uma solução de melhoria, podendo optar por implementar outro método de segurança além do WEP.

Dessa forma, baseado na necessidade de implementação de segurança, este estudo propõe um método de segurança baseado na criação de redes privadas virtuais. Para realizar a criação de uma VPN será utilizado o software OpenVPN, onde será necessária a utilização de um servidor capaz de prover acesso à rede. Primeiramente será montada uma topologia com um servidor, um host e um intruso, onde serão realizados testes para comparação dos resultados obtidos anteriormente sem a utilização do servidor.

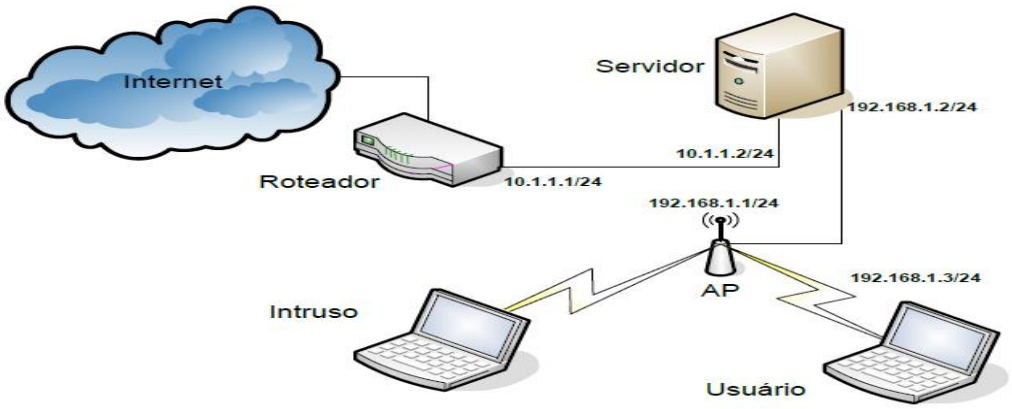

Figura 74: Ambiente de Teste. Fonte: Elaboração Própria (VISIO, 2014).

Para a realização dos testes foram utilizados os seguintes itens: Um intruso possuindo um notebook com interface de rede sem fio configurada em modo promíscuo; Um host com notebook com interface de rede sem fio configurada com o IP local 192.168.1.3; Um AP, configurado com o IP local 192.168.1.1. Um servidor com duas interfaces configuradas como: Interface de rede sem fio com o IP local 192.168.1.2; interface de rede LAN com o IP 10.1.1.2 - Internet; Um roteador configurado com o IP 10.1.1.1.

É necessária uma série de passos para a realização da configuração, segue um passo a passo, a começar pela instalação do software a ser utilizado: Instalando o sistema OpenVPN no servidor: # apt-get install openvpn; Criando certificados e chaves: Copiando os scripts do OpenVPN: (# cp -r /usr/share/doc/openvpn/examples/easy-rsa/2.0/. /etc/openvpn/); Acessando o diretório copiado: (# cd /etc/openvpn/easy-rsa/); Carregando as informações de configuração: (# source ./vars); Limpando todas as variáveis existentes: (# source ./clean-all); Criando uma autoridade certificadora: (# ./build-ca); A execução do comando resultará na criação dos arquivos: ca.crt - Certificado público da CA, ca.key - Certificado privado da CA, Serial - Controle do número serial das chaves geradas pela CA, index.txt - Controle das chaves geradas pela CA. (a) Criando o certificado e a chave do servidor: # ./build-key-server sever (nome do servidor), A execução do comando resultará na criação dos arquivos: server.crt - Certificado público do servidor, server.key - Certificado privado do servidor, Criando o certificado e a chave do cliente: # ./build-key client1 (nome do cliente). A execução do comando resultará na criação dos

arquivos: client1.crt - Certificado público do cliente, client1.key - Certificado privado do cliente, Gerando os parâmetros necessários do Diffie Hellman. # ./build-dh.

A execução do comando resultará na criação dos arquivos: dh1024.pem - Arquivo que proporcionará a troca de informação entre o servidor e o cliente em um ambiente não seguro, sem comprometer a segurança. Além disso, configurando o OpenVPN Server: (a) Criar o arquivo de configuração do OpenVPN e de log, isto é, # touch /etc/openvpn/server.conf, # touch /var/log/openvpn.log e (b) Editar o arquivo inserindo as seguintes linhas de configurações: # vim /etc/openvpn/server.conf, server.conf, dev tun, tls-server, proto udp, ca /etc/openvpn/easy-rsa/keys/ca.crt, cert /etc/openvpn/easy-rsa/keys/server.crt, key /etc/openvpn/easy-rsa/keys/server.key, dh /etc/openvpn/easy-rsa/keys/dh1024.pem, ifconfig 192.168.11.1 255.255.255.0, ifconfig-pool 192.168.11.2 192.168.11.254 255.255.255.0, comp-lzo, persist-tun, persist-key, float, verb 3, log /var/log/openvpn.log. Onde: dev tup - Dispositivo virtual utilizado para vpn; tls-server - Permitir o uso de conexões SSL/TLS tipo servidor; proto udp – Utilização do protocolo UDP para transporte dos dados; ca - Certificado público da CA; cert - Certificado público do servidor; key - Certificado privado do servidor; dh - Diffie Hellman; ifconfig - IP utilizado no túnel da VPN; ifconfig-pool - Pools de ip reservados para os clientes; comp-lzo - Habilita a compressão dos dados; persist-tun - Mantém a interface tun configurada mesmo após um reset na aplicação OpenVPN; persist-key - Mantem a chave carregada mesmo após um reset na aplicação OpenVPN; float - Caso ocorra alteração no IP o túnel permanecerá estabelecido; verb 3 - Nível de detalhes das conexões; log - Arquivo de log.

E configurando o OpenVPN client: (a) Para que seja possível a comunicação e configuração do OpenVPN client, é necessário que sejam copiados de modo seguro do servidor os arquivos: ca.crt, client1.crt, client1.key, dh1024.pem. Para criar o arquivo de configuração do OpenVPN client. E dentro do diretório c:/Arquivos de Programas/OpenVPN/config/, Inserir os arquivos de configuração copiados do servidor e criar um novo arquivo com o nome: client1.ovpn, dev tap, tls-client, proto udp, remote 10.1.1.2, ca ca.crt, cert client1.crt, key client1.key, dh dh1024.pem, comp-lzo, persist-tun, persist-

key, float e verb 3. Onde: dev tap - Dispositivo virtual criado no Windows; tls-client - Permitir o uso de conexões SSL/TLS tipo cliente e remote - IP remoto do servidor.

Para criar a rota no servidor, temos que (a) Criar a rota de entrada via VPN para saída internet: # iptables -t nat -A POSTROUTING -s 192.168.11.0 -o wlan0 -j MASQUERADE; # echo “1” > /proc/sys/net/ipv4/ip_forward. Onde: iptables - Aplicação utilizada no linux 2.4.x, baseado em regras para realização de filtro dos pacotes trafegados pela rede; echo “1” > /proc/sys/net/ipv4/ip_forward - Comando utilizado para ativar o encaminhamento dos pacotes de uma interface para outra, conforme Figura 8.

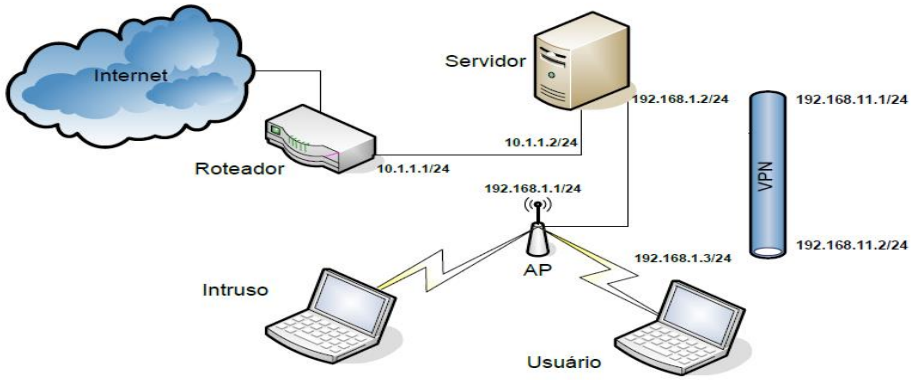

Figura 85: Ambiente de Teste com VPN – OpenVPN. Fonte: Elaboração Própria (VISIO, 2014).

E para iniciar o OpenVPN server + client. Iniciar o OpenVPN server no servidor: # /etc/init.d/openvpn restart; Iniciar o OpenVPN client no cliente: Acessar o diretório c:/Arquivos de Programa/OpenVPN/config/. E selecionar o arquivo client1.ovpn e executar: Start OpenVPN on This Config File. E acessar as configurações de rede padrão e inserir o gateway 192.168.11.1 (ip da vpn do servidor remoto), conforme mostrado na Figura 8.

E finalmente, depois de finalizar todo o processo de instalação e configuração do software OpenVPN, foram realizados testes onde foram utilizadas as mesmas ferramentas e os mesmos princípios para invadir a rede. O resultado da análise de tráfego realizada pela ferramenta *tcpdump* em uma rede WEP, onde antes era possível ler e capturar todo o tráfego é mostrado na Figura 9.

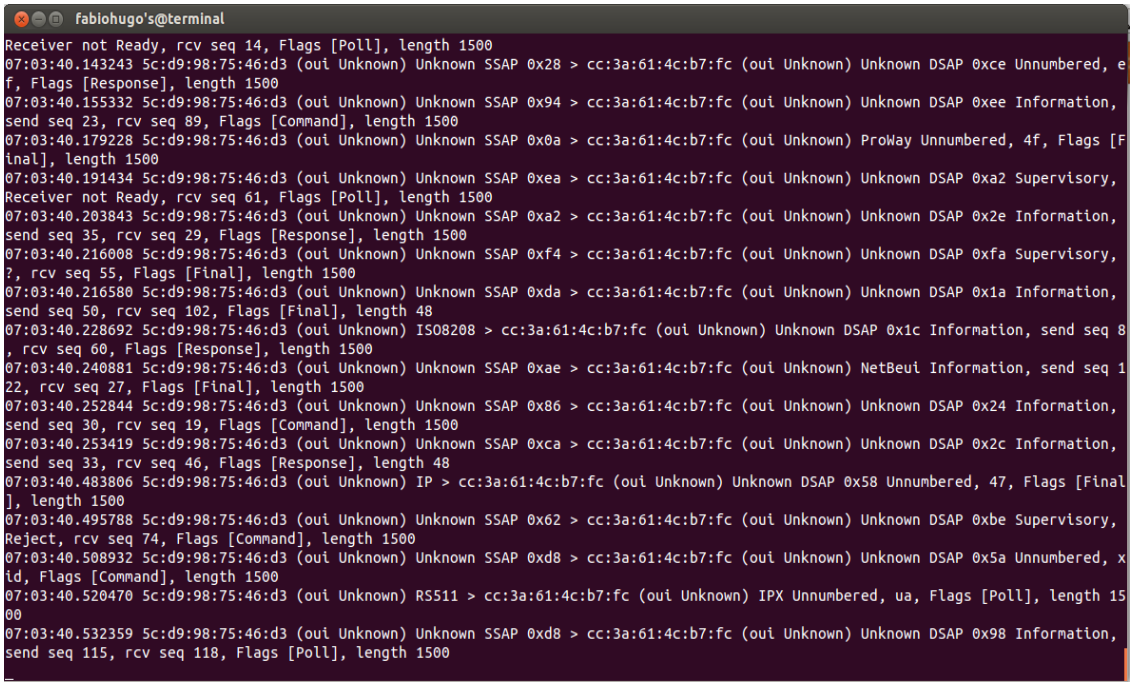

Figura 96: Tráfego na Rede Verificado com o Tcpdump. Fonte: Elaboração Própria (2014).

Nessa aplicação foi utilizado apenas um AP, dada a necessidade de teste com a presença do servidor, o que torna difícil a realização de testes com diferentes proprietários. Foi comprovado com os testes nas redes WEP que o sistema de VPN não é capaz de fornecer mais segurança quanto à quebra das chaves, porém em termos de privacidade as redes privadas virtuais alcançaram seu objetivo. Destarte, uma forma de identificar a privacidade são as aplicações *Unknown,* mostrando que não é possível localizar o tráfego trocado entre host/servidor.

5. CONSIDERAÇÕES FINAIS

Os avanços tecnológicos proporcionaram o desenvolvimento das redes sem fio, as quais rapidamente ganharam força no mercado e conquistaram os diversos utilizadores das redes com cabeamento, visto que proporcionam uma série de vantagens que as redes convencionais não podem oferecer, por exemplo, mobilidade, flexibilidade e abrangência, em que é possível o acesso à rede em locais de difícil acesso físico. E com o desenvolvimento dessas redes, vários dispositivos incorporaram essa tecnologia, a qual tem crescido e se desenvolvido bastante, aprimorando sua capacidade e solucionando seus problemas, onde a segurança é o maior de seus problemas.

Dessa forma, os estudos realizados sobre os protocolos de segurança das redes sem fio, proporcionaram um melhor entendimento de como funcionam os diferentes métodos de criptografia utilizados para garantir o sigilo, a autenticidade e a integridade das informações trafegadas nessas redes. Com isso, foi possível entender os pontos de vulnerabilidade existentes nesses protocolos e entender também a necessidade de se desenvolver novos protocolos de segurança para eliminar as condições de riscos existentes nas redes Wi-Fi.

No estudo de caso realizado, para os casos em que a segurança da rede possuía configuração padrão ou má configurada, foi possível observar que com pouco conhecimento de informática, uma pessoa pode ser capaz de realizar a invasão da rede e, em alguns casos, conseguir fazer a captura de informações presentes na rede. Nesse sentido, pode-se concluir que é indispensável à realização da configuração na segurança da rede diferente do padrão, melhor ajustada, e a utilização de outro método de segurança aplicado às redes Wi-Fi, além dos protocolos padrões oferecidos pela rede. E a solução utilizada, a criação de VPNs, não oferece maior segurança no acesso indevido à rede, porém teve resposta nos testes realizados para tentar obter algum tipo de informação na rede, demonstrando segurança adequada quanto à privacidade das informações trafegadas na rede. Porém, deve ser ressaltado, que não são todas as aplicações VPNs seguras, visto que esse método depende dos protocolos utilizados em sua implantação.

Portanto, apesar das redes Wi-Fi apresentarem vulnerabilidades, não se pode dizer que essas redes são totalmente vulneráveis, uma vez que com o avanço no desenvolvimento de melhorias na sua segurança, não é qualquer pessoa, com qualquer equipamento, que consegue realizar um ataque a uma rede. Uma vez que a rede seja configurada de forma adequada, pode proporcionar uma boa segurança, restringindo a possibilidade de ataques às pessoas com alto grau de conhecimento. Os vários relatos dos riscos e ameaças às redes Wi-Fi, fazem os desenvolvedores dessas redes disponibilizem melhorias na segurança e alguns dos métodos utilizados, anteriormente, para invadir uma rede não tenham mais efeito. Portanto, as ferramentas de ataques estão sendo desenvolvidas e aprimoradas. E a

segurança das redes também está em desenvolvimento para acabar com os riscos e ameaças existentes.

6. REFERÊNCIAS

AGUIAR, Daniel. **Estudo Sobre Crimes Praticados na Internet com o Uso do Computador**. 2009. 104 f. Trabalho de Conclusão de Curso (Tecnologia em Informática com Ênfase em Gestão de Negócio) – Faculdade de Tecnologia da Zona Leste, São Paulo. 2009.

AIRCRACK-NG. **Aircrack-ng Installation**. Disponível em: <http://www.aircrack-ng.org/install.html>. Acesso em: 25/01/2014.

ALBUQUERQUE, Alessandro. **Estudo de Métodos de Proteção de Redes Wireless**. 2008. 72 f. Trabalho de Conclusão de Curso (Pós-Graduação *Lato-Senso* em Redes de Computadores – Configuração e Gerenciamento de Ativos) – Universidade Tecnológica Federal do Paraná, Medianeira. 2008.

ALVES, Francinildo, et al. **Análise de Vulnerabilidades em Redes sem Fio**. 2010. 57 f. Trabalho de Conclusão de Curso – Faculdade Integrada do Ceará (Curso Tecnólogo em Rede de Computadores), Fortaleza. 2010.

ALVES, Nilton; BRAGA, Nilton; CARNEIRO, Leonardo. **Rede de Computadores**. 1998. 47 f. Nota Técnica.

AMORAS, Romulo; BRABO, Gustavo; PEREIRA, Carlos. **Segurança em Redes Wireless Padrão IEEE802.11b: Protocolos WEP, WPA e Análise de Desempenho**. 2004. 78f. Trabalho de Conclusão de Curso – Universidade da Amazônia UNAMA (Curso Ciência da Computação), Belém. 2004.

AMORIM, Fábio. **Implantação de Redes Wireless para Melhoria do Controle e Monitoramento de Automação Industrial.** 2011. 63 f. Trabalho de Conclusão de Curso (Curso de Tecnologia em Redes de Computadores) – Faculdade de Tecnologia de São José dos Campos FATEC, São José dos Campos, 2011.

BEZERRA, Dinarde; SOUSA, Gustavo. **Protocolos Criptográficos**. 2008. 74 f. Trabalho de Conclusão de Curso – Faculdade de Tecnologia Termomanica (Curso de Tecnologia em Análise e Desenvolvimento de Sistemas), São Bernardo do Campo. 2008.

BORGES, Fábio; CUNHA, Gerson; FAGUNDES, Bruno. **VPN: Protocolos e Segurança**. S/D. 10 f. Artigo Científico – Universidade Católica de Petrópolis, Rio de Janeiro. S/D.

BORTOLUZZI, Dayna; CUNHA, Erivelto; SPECIALSKI, Elizabeth. **An Extended Model for TCPIP Architecture**. 2004. 5 f. Artigo Científico – Universidade Federal de Santa Catarina, Santa Catarina. 2004.

BROWN, EDWIN. **802.1X PORT-BASED AUTHENTICATION**. NOVA YORK. AUERBACH PUBLICATIONS, 2007.

CERT.BR. **Estatística de Incidentes Reportados ao Cert.br**. Disponível em: <http://www.cert.br/stats/incidentes/>. Acesso em 10/12/2013.

CYSCO SYSTEMS. **Internetworking Technologies Handbook**, Cisco Press , 2004.

CYSCO SYSTEMS, INC. **VPN**. Disponível em: <http://www.cisco.com/web/BR/solucoes/pt_br/vpn/index.html>. Acesso em: 10/02/2014.

GOMES, Luís. **Fundamentos de Rede**. 2007. 85 f. Trabalho Acadêmico – Escola Agrotécnica Federal de São João Evangelista (Curso Técnico em Informática), São João Evangelista. 2004.

IEEE COMPUTER SOCIETY. **Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications**. Disponível em: <http://standards.ieee.org/getieee802/download/802.11-2012.pdf>. Acesso em: 12/01/2014. ISBN 978-0-7381-7245-3 STDPD97218.

JARA, Diego; AUGUSTO, Felipe. **Segurança em Redes Sem Fio.** 2011. 12 f. Artigo Científico – Universidade Nove de Julho, São Paulo, 2011.

KARNIK, Ankush; PASSERINI, Katia. **Wireless Network Security - A Discussion From a Business Perspective.** 2005. 7 f. Artigo Científico.

LINUX, UBUNTU. **Ubuntu 13.10 Saucy Salamander**. Disponível em: <http://www.ubuntu.com/download/desktop>. Acesso em: 28/11/2013.
MARX, Tiago. **Do Projeto à Implantação de Redes Sem Fio.** 2008. 50 f. Trabalho de Conclusão de Curso (Curso Sistemas de Informação) – Universidade do Oeste de Santa Catarina, São Miguel do Oeste, 2008.

MENDES, Douglas. **Redes de Computadores: Teoria e Prática**. São Paulo: Novatec, 2007.

METAGEEK LLC. **inSSIDer Home.** Disponível em: <http://www.metageek.net/products/inssider/>. Acesso em: 05/01/2014.

MIRANDA, Anibal. **Introdução às Redes de Computadores**. Vitória: ESAB, 2008.

MORAES, Alexandre Fernandes De. **Redes Sem Fio**. São Paulo: Erica, 2011.

OPENVPN TECHNOLIGES, INC. **OpenVPN Community Software**. Disponível em: <http://openvpn.net/index.php/open-source/overview.html/>. Acesso em: 10/01/2014.

OPPLIGER, Rolf. **SSL and TLS: Theory and Practice**. Norwood: Artech House, 2009.

RAMASWAMY, Raju. **A Security Architecture and Mechanism for Data Confidentiality in TCP/IP Protocols**. 1990. 11 f. Artigo Científico – University of Missouri, Kansas City, 1990.

RANJINI, T; YAMUNA, R. **Wireless Technology**. 2011. 4 f. Artigo Científico – Kongu Engineering College, Coimbatore, 2011.

REAVER SYSTEM SOLUTIONS. **WiFi Protected Setup**. Disponível em: <http://www.reaversystems.com/>. Acesso em: 15/02/2014.

RED LINE SOFTWARE. **Example of VPN Tunnel Configuration**. Disponível em: <http://www.redline-software.com/eng/support/docs/winroute/ch12s05.php>. Acesso em 09/01/2014.

RUFINO, Nelson Murilo De Oliveira. **Segurança em Redes Sem Fio**. São Paulo: NOVATEC, 2011.

STALLINGS, William. **Criptografia e Segurança de Redes**. São Paulo: Pearson, 2012.

STALLINGS, William. **IEEE 802.11: Moving Closer to Practical Wireless LANs**. 2001. 7 f. Artigo Científico. 2001.

TANENBAUM Andrew S. **Redes de Computadores**, Elsevier, 2003 – 4. Edição.

TCPDUMP & LIBPCAP. **Tcpdump Home**. Disponível em: <http://www.tcpdump.org/>. Acesso em 20/01/2014.

TELECO. **Redes WLAN de Alta Velocidade I: Características**. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialredeswlanI/default.asp>. Acesso em 08/11/2013.

TRINTA, MACEDO. **Um Estudo Sobre Criptografia e Assinatura Digital**. Disponível em: <http://www.di.ufpe.br/~flash/ais98/cripto/criptografia.htm>. Acesso em 26/12/2013.

VISIO, MICROSOFT CORP. **Microsoft Visio Professional 2013**. Disponível em: <http://office.microsoft.com/en-us/visio/>. Acesso em: 20/02/2014.

VIVA O LINUX. **VPN em Linux com OpenVPN**. Disponível em: <http://www.vivaolinux.com.br/artigo/VPN-em-Linux-com-OpenVPN/>. Acesso em: 08/01/2014.

WI-FI ALLIANCE. **Wi-Fi**. Disponível em: <http://www.wi-fi.org/>. Acesso em: 15/01/2014.

WINDOWS 7, MICROSOFT CORP. **Windows 7 Home Premium**. Product Key: TC469 – PPBGY – 893DB – QDC6Q – 8C9Y7.

WINDOWS 8, MICROSOFT CORP. **Microsoft Windows 8**. Product ID: 00179 – 40493 – 83959 – AAOEM.

WORD, MICROSOFT CORP. **Microsoft Word 2013**. Disponível em: <http://office.microsoft.com/en-us/word/>. Acesso em: 21/10/2013.

ZHENG, PEI. ET AL. **WIRELESS NETWORKING COMPLETE**. BURLINGTON. MORGAN KAUFMANN, 2009.

ZIMMERMANN, Hubert. **OS1 Reference Model-The IS0 Model of Architecture for Open Systems Interconnection**. 1980. 8 f. Artigo Científico. 1980.