FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Hugo Henrique Genaro

ANÁLISE DA SEGURANÇA EM REDES SEM FIO PÚBLICAS

Americana, SP

2016

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Hugo Henrique Genaro

ANÁLISE DA SEGURANÇA EM REDES SEM FIO PÚBLICAS

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do Prof. Dr. José Luis Zem.

Área de concentração: Segurança da Informação.

Americana, SP

2016

G288a GENARO, Hugo Henrique

Análise da segurança em redes sem fio públicas / Hugo Henrique Genaro. – Americana: 2016.

48f.

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

Orientador: Prof. Dr. José Luis Zem

1. Wireless – rede de computadores I. ZEM, José Luis II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 681.519

Hugo Henrique Genaro

ANÁLISE DA SEGURANÇA EM REDES SEM FIO PÚBLICAS

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.

Área de concentração: Segurança da Informação.

Americana, 10 de dezembro de 2016.

Banca Examinadora:

José Luis Zem (Presidente)
Doutor
FATEC Americana

Daniele Junqueira Frosoni (Membro)
Especialista
FATEC Americana

Rogério Nunes de Freitas (Membro)
Especialista
FATEC Americana

AGRADECIMENTOS

Ao Prof. Dr. José Luis Zem pela orientação, compreensão e incentivo dispensado durante o desenvolvimento deste trabalho.

A todos professores que contribuíram diretamente ou indiretamente no desenvolvimento do trabalho.

Aos meus pais, pelo incentivo e apoio.

DEDICATÓRIA

À

Minha Família

Em especial aos meus pais:

Devanir e Janete.

RESUMO

O presente trabalho tem como objetivo realizar uma análise dos métodos de segurança utilizados em redes sem fio públicas, entende-se como rede sem fio pública uma rede que qualquer pessoa possa ter acesso, esta análise foi feita através de uma metodologia qualitativa de pesquisa de campo. O presente texto conceitua a segurança da informação, rede sem fio envolvendo sua definição, classificação e padrões mais utilizados, sendo eles 802.11 (Wi-Fi), 802.15 (Bluetooth) e 802.16 (WiMAX). Também conceitua aspectos relacionados à segurança em rede sem fio, envolvendo as ameaças e vulnerabilidades que uma rede sem fio podre sofrer, os tipos de ataques mais comuns a redes sem fio e técnicas seguras utilizadas para prevenção destas ameaças, vulnerabilidades e ataques. Foi realizada a análise em quatros ambientes, sendo um ambiente acadêmico, um ambiente público, um ambiente comercial e um ambiente de saúde onde foi testado se é possível realizar a identificação de todos nós da rede, realizar a captura de pacotes destes nós, mostrando uma vulnerabilidade que pode ser explorada através disto, e realizar uma varredura na rede com objetivo de descobrir portas e serviços abertos nestes mesmos nós. Os resultados dos testes mostraram que foi possível descobrir, capturar pacotes e varrer portas e serviços abertos de todos os nós apenas em três ambientes, e que o ambiente público foi o mais seguro analisado.

Palavras Chave: segurança da informação; rede de computadores; rede sem fio.

ABSTRACT

The present work has as I aim to carry out an analysis of the methods of security used in public wireless network, it understands itself how wireless public network a network that anyone could have access, this analysis was done through a qualitative methodology of field research. The present text conceptualizes the information security, wireless envolving his definition, classification and more used standards, when they are 802. 11 (Wi-Fi), 802. 15 (Bluetooth) and 802. 16 (WiMAX). Also it conceptualizes safety aspects in wireless network, involving the threats and vulnerabilities that a wireless network will suffer, the types of commoner attacks to wireless network and safe techniques used for prevention of these threats, vulnerabilities and attacks. It was carried out the analysis in four enviroments, being an academic enviroment, a public enviroment, a commercial enviroment and an enviroment of health, where it was tested if it is possible to carry out the identification of network nodes, carry out the capture of packets of these nodes, showing a vulnerability that can be explored through this, and carry out a sweep in the network with objective to discover ports and services opened in the same nodes. The results of the tests showed that it was possible to discover, to capture packets and to sweep ports and open services of all the nodes only in three enviroments, and that the public enviroment was the safest analysed.

Keywords: *information security; computer network; wireless network.*

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AP	Ponto de acesso
BSS	Conjunto Básico de Serviço
CERT	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
DS	Sistema de Distribuição
ESS	Conjunto de Serviços Estendidos
GHz	*Gigahertz*
HTTP	Protocolo de Transferência de Hipertexto
HTTPS	Protocolo de Transferência de Hipertexto Seguro
IEEE	Instituto de Engenheiros Eletricistas e Eletrônicos
IMAP	Protocolo de Acesso a Mensagem da Internet
MAC	Controle de Acesso ao Meio
Mbps	*Megabit* por segundo
NNTP	Protocolo de Transferência de Notícias na Rede
POP3	Protocolo dos Correios
RFC	Pedido de Comentários
SMTP	Protocolo Simples de Envio de E-mail
SNMP	Protocolo Simples de Gerenciamento de Rede
SSH	*Shell* Seguro
SSID	Identificador de Conjunto de Serviços
SSL	Camada de Soquetes Segura
STA	Estação sem Fio
WECA	*Wireless Ethernet Compatibility Alliance*
WEP	Privacidade Equivalente à de Redes com Fio
WiMAX	Interoperabilidade Mundial para Acesso de Micro-Ondas
WLAN	Rede Local sem Fio
WMAN	Rede Metropolitana sem Fio
WPA	Acesso Protegido a Wi-Fi
WPA2	Acesso Protegido a Wi-Fi 2
WPAN	Rede Pessoal sem Fio

WWAN Rede de Longa Distância sem Fio

1 INTRODUÇÃO

O tema desta monografia é Análise da Segurança de Redes, em particular as redes sem fio públicas. As redes sem fio já são muito comuns hoje em dia devido à grande expansão de uso da Internet, o avanço das tecnologias de rede e equipamentos com preços mais acessíveis. Atualmente empresas e pessoas não conseguem ficar sem acesso à Internet devido ao trabalho, comunicação, compras e diversão. Com o advento da Internet, os locais estão se adaptando ao uso de redes sem fio, beneficiando seus clientes com o acesso à mesma.

A segurança é um fator muito importante em uma rede de computadores, ainda mais em uma rede sem fio pública onde qualquer um pode ter acesso, porém muitos usuários comuns não sabem disso. A melhor maneira de se conhecer a segurança nesse tipo de rede é saber como funciona e com isso os usuários podem reconhecer se a rede que estão conectados é confiável ou não.

O objetivo geral deste trabalho foi analisar a segurança de algumas redes sem fio públicas, realizando uma varredura nas mesmas para coletar de dados e analisando-os, foi possível identificar algumas vulnerabilidades presentes e apresentar um método de segurança eficaz afim de reduzir as vulnerabilidades encontradas e outras que poderão surgir.

Como objetivos específicos buscou-se explicar como funciona a segurança de uma rede sem fio; identificar os riscos, as ameaças e as vulnerabilidades que podem ter em uma rede sem fio; além de identificar os riscos que um usuário pode correr estando conectado à essa rede e apresentar os métodos seguros para configuração da mesma de modo que as informações do usuário não fiquem vulneráveis.

A pesquisa caracteriza-se como qualitativa. Foi realizada uma pesquisa de campo de forma que pode ser analisada a segurança de redes sem fio públicas, pois com a pesquisa de campo pode se comprovar a veracidade dos dados apresentados.

O trabalho foi estruturado em cinco capítulos, sendo que o segundo conceitua informações sobre segurança da informação, envolvendo seus três pilares principais, sendo eles a confidencialidade, a integridade e a disponibilidade; rede sem fio, considerando suas classificações e seus padrões, sendo eles o padrão 802.11 (Wi-Fi), 802.15 (Bluetooth) e 802.16 (WiMAX) e segurança de rede sem fio, apresentando as ameaças e vulnerabilidades que uma rede sem fio pode sofrer, os tipos de ataques

existentes a redes sem fio e também as técnicas seguras utilizadas para mitigar essas ameaças, vulnerabilidades e ataques.

O terceiro apresenta os cenários, sendo um ambiente acadêmico, um ambiente público, um ambiente comercial e um ambiente de saúde; e os testes que foram realizados nestes ambientes; o quarto discute os resultados obtidos a partir dos testes realizados no capítulo anterior, e por fim, o quinto capítulo se reserva às considerações finais.

2 REFERENCIAL BIBLIOGRÁFICO

Neste capítulo serão apresentados conceitos e teorias referentes a segurança da informação, redes sem fio e segurança em redes sem fio.

2.1 Segurança da Informação

De acordo com Departamento de Segurança da Informação e Comunicações – DSIC (2009), a segurança da informação é:

> "Proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão e a modificação desautorizada de dados ou informações, armazenados em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento".

Segundo Semôla (2014), a segurança da informação tem como objetivo a preservação de três princípios base: confidencialidade, a informação deve ser protegida segundo o grau de sigilo de seu conteúdo, limitando seu acesso e uso apenas às pessoas autorizadas; integridade, a informação deve ser mantida no mesmo estado quando foi disponibilizada pelo seu proprietário, visando protegê-la contra alterações indevidas, intencionais ou acidentais; e disponibilidade**,** a informação deve estar disponível aos que necessitam dela para quaisquer fins.

Tanenbaum (2010) também aponta os mesmos como os três princípios base da segurança da informação, com conceitos similares, sendo: confidencialidade, manter os dados em segredo e estes dados podem ser disponibilizados apenas por pessoas com permissões especificadas, também deve-se garantir que pessoas sem permissões não tenho acesso nenhum; integridade, os dados só podem ser modificados perante a permissão do proprietário, nessa modificação consta também remoção e inclusão de dados além de alteração; e disponibilidade; ninguém pode perturbar os dados ou informações com intenções de deixá-los indisponíveis. O mesmo autor alega ainda que cada princípio tem uma meta e enfrenta uma ameaça conforme a Tabela 1.

Tabela 1: Metas e ameaças de SI.

Meta	Ameaça
Confidencialidade de dados	Exposição de dados
Integridade de dados	Manipulação de dados
Disponibilidade do sistema	Recusa de serviços

Fonte: Tanenbaum (2010)

Semôla (2014), afirma que além dos três princípios básicos, deve-se levar em consideração aspectos que são essências na prática da segurança da informação como a autenticação, modo de identificação e reconhecimento dos elementos que estão em comunicação; e conformidade, modo de garantia do cumprimento de obrigações empresariais e com aspectos legais e regulatórios.

Além desses aspectos essenciais, o mesmo autor também aponta outros aspectos que são associados aos essenciais. Entre eles estão a autenticidade, garantia de que as entidades identificadas durante a realização de uma comunicação são realmente quem dizem ser; a irretratabilidade ou não repúdio, garantia de que a informação possua a identificação do emissor; a legalidade, garantia de que a informação é legal perante as leis; a privacidade, garantia de privacidade da informação ou usuário; e a auditoria, garantia de que nos recursos utilizados existem evidências com informações de quem uso a fins de identificação.

2.2 Rede sem Fio

Uma rede sem fio é uma rede de computador que não utiliza de uma infraestrutura cabeada para realizar a transmissão de dados. Ramalho (2014) afirma que esse tipo de rede utiliza de propagação de radiação eletromagnética, como radiofrequência ou infravermelho, para transmitir os dados entre os dispositivos.

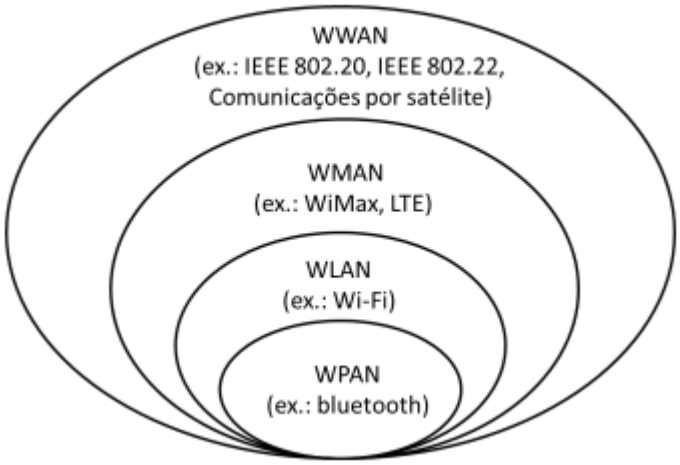
Segundo Souza, Silva e Guimarães (2009), a primeira rede sem fio surgiu em 1970 e sua função era ligar quatro ilhas onde estavam localizados os *campi* da universidade do Havaí.

De acordo com Ramalho (2014), essa rede possuía um sistema chamado ALOHA que foi desenvolvido por Abramson, também em 1970, o ALOHA tinha como objetivo resolver problemas de alocação de canais e utilizava da radiofrequência para realizar a comunicação.

A princípio, as redes sem fio utilizavam de um transmissor e um receptor infravermelho para a transmissão de dados que causava uma baixa qualidade e confiabilidade. A partir da década de 90 as redes sem fios começaram a utilizar da transmissão via ondas de rádio eletromagnéticas, pelo fato de que processadores e outras tecnologias evoluíram e conseguiram gerenciar os dados que trafegam na rede.

O mesmo autor diz que, a classificação de uma rede sem fio ocorre de acordo com sua área de alcance. Divide-se em quatro classificações: *Wireless Personal Area Network* (WPAN), *Wireless Local Area Network* (WLAN), *Wireless Metropolitan Area Network* (WMAN) e *Wireless Wide Area Network* (WWAN). A Figura 1 simboliza a diferença de alcance entre as quatros classificações de redes citadas anteriormente.

Figura 1: Classificação de redes sem fio



Fonte: Selada (2008) *apud* Ramalho (2014)

De acordo com IEEE 802.15.4-2006 (2006) *apud* Steinhauser (2013, p. 4):

> “As WPANs são utilizadas para transmitir informações a distâncias relativamente curtas, envolvendo pouca estrutura, permitindo a implementação de soluções eficazes e de baixo custo e que ainda, pode ser implementado por uma ampla gama de dispositivos”.

Este tipo, normalmente, tem um alcance de 10 metros com uma velocidade de transmissão de 2 Mbps. Um exemplo deste tipo de classificação de rede é o Bluetooth (802.15) que será conceituado na seção 2.2.3.2.

Uma WLAN é uma rede local sem fio que utiliza de ondas de rádio para transmissão de dados e que atingem distâncias entre 30 e 500 metros. Uma rede deste tipo é o Wi-Fi (802.11) que será conceituada na seção 2.2.3.1.

Segundo Ramalho (2014), uma rede WMAN é um conjunto de rede locais conectadas que atinge grandes distâncias. Um exemplo deste tipo de classificação de rede são as redes WiMAX (802.16) que será conceituada na seção 2.2.3.3.

Uma WWAN interliga redes de alcance menor por uma maior área geográfica cobrindo milhares de quilômetros. Um exemplo atual deste tipo de classificação de rede são as redes de celulares, como GSM, 3G e 4G.

2.2.3 Padrões de rede sem fio

O IEEE definiu padrões para redes sem fio, onde definem as tecnologias e frequências a serem utilizadas. Entre os padrões de rede sem fio, os mais difundidos são os padrões 802.11, 802.15 e 802.16.

2.2.3.1 802.11 (Wi-Fi)

De acordo com Rufino (2015), Souza, Silva e Guimarães (2009), em 1997 a IEEE criou o padrão 802.11 que define especificações de como deve ser feito a comunicação entre os dispositivos utilizados.

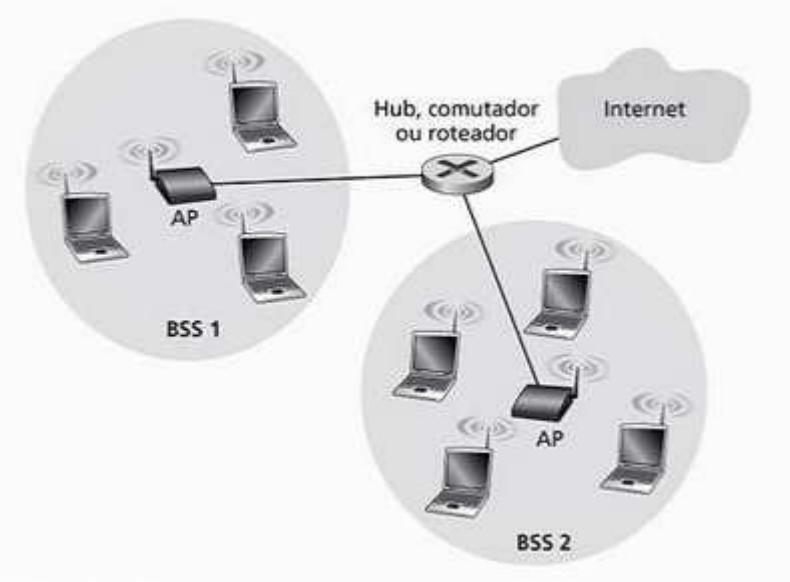
Em 1999, com a união das empresas 3Com, Nokia, Lucent Technologies e Symbol Technologies foi criada a Wireless Ethernet Compatibility Alliance (WECA), renomeada para Wi-Fi Alliance em 2003, com o objetivo de desenvolver uma tecnologia baseada no padrão 802.11 e com essa união foi definido o Wi-Fi.

Segundo Vilela (2014), Kurose e Ross (2014), a arquitetura do padrão 802.11 é formada pelos componentes a seguir e que podem ser vistos na Figura 2:

• *Basic Service Set* (BSS) é a componente base de uma rede 802.11, em um BBS fica concentrado um grupo de estações;
• *Access Point* (AP) é o dispositivo que fornece conexão à rede para as demais estações sem fio;
• *Wireless Station* (STA) é qualquer dispositivo que tenha acesso a rede sem fio;

• *Distribution System* (DS) envia os dados entre as STAs, BSSs e consequentemente para outras redes ou para à Internet.
• *Extended Service Set* (ESS) é formado por um conjunto de BSSs conectados por um DS.
• *Service Set Identifier* (SSID) é o nome da rede.

Figura 2: Exemplo da arquitetura do padrão 802.11



Fonte: Kurose e Ross (2014)

Segundo Gast (2005) *apud* Vilela (2014), uma rede no padrão 802.11 pode ser dividida em: AD HOC e Infraestrutura.

A rede **AD HOC**, de acordo com Rufino (2015) e Tanenbaum (2011), é uma rede que não precisa de um concentrador ou de um ponto de acesso, ou seja, um dispositivo pode se conectar a outro sem a necessidade de um intermediador, conforme a Figura 3.

Figura 3: Rede ad hoc

Fonte: Rufino (2014)

A **rede Infraestrutura** segundo Rufino (2015) e Tanenbaum (2011), é uma rede que precisa de um concentrador ou um ponto de acesso, ou seja, os dispositivos precisam se conectar a um intermediador para conseguirem realizar a comunicação entre os mesmos, conforme a Figura 4.

Figura 4: Rede infraestrutura

Fonte: Rufino (2014)

No padrão **802.11**, a velocidade de transmissão é de 2Mbps e utiliza a frequência de 2,4GHz. Opera nas camadas física e enlace do modelo de referência ISO/OSI (TANENBAUM, 2011), como citado anteriormente o tipo de classificação de rede utilizada por este padrão é o WLAN.

Segundo Rufino (2015), com o avanço tecnológico, houve a necessidade de novas tecnologias, então surgiram novas extensões do padrão 802.11 que incluem novas características técnicas e operacionais. Sendo eles:

O padrão **802.11b** foi definido em 1999 com parâmetros semelhantes ao das redes Ethernet, opera em uma velocidade de 11 Mbps, utiliza 14 canais na frequência de 2,4GHz, e possui um número máximo de 32 clientes que podem estar conectados. Também descreve como deve ser a implementação em redes WLAN e o protocolo de segurança WEP.

O padrão **802.11a** foi definido com o objetivo de resolver os problemas presentes nos padrões 802.11 e 802.11b, opera com a velocidade de transmissão de 54Mbps e com frequência de 5GHz. Também teve o número de clientes aumentado para 64 e especifica as camadas física e enlace de dados do modelo de referência ISO/OSI (TANENBAUM, 2011) para redes sem fio que operam na frequência de 5GHz.

O principal problema encontrado nesse padrão é a compatibilidade com os dispositivos existentes, já que os mesmos foram desenvolvidos utilizando com base os padrões anteriores.

O padrão **802.11g** foi desenvolvido utilizando o padrão 802.11a como base, onde opera com a velocidade de transmissão a 54Mbps na frequência de 5GHz. Porém resolve o principal problema em relação ao padrão que tem como base, operando com dispositivos tanto de frequência de 2,4GHz quanto de 5GHz na mesma rede.

O padrão **802.11i** foi definido com o objetivo de aumentar a segurança, além do protocolo WEP também estão presente nesse padrão o protocolo WPA e o WPA2. Sua velocidade de transmissão e frequências utilizadas são as mesmas do padrão 802.11a.

O padrão **802.11n** foi definido com objetivo de aumento significativo na velocidade de transmissão de redes sem fio, de 100 a 500Mbps. Este também é conhecido como *World Wide Spectrum Efficiency* (WWiSE). Assim como o padrão 802.11g, este padrão pode trabalhar em ambas frequências. Outro ponto importante a respeito deste padrão é que todas as frequências anteriores são suportadas, ou seja, se um dispositivo utilizar do padrão 802.11b ou os demais, ele irá funcionar com um transmissor que utiliza do padrão 802.11n.

O padrão **802.11ac** foi definido com objetivo de melhorar o sinal de transmissão e também entregar taxas de velocidade de transmissão de 433Mbps a 1.3Gbps, opera na faixa de frequência de 5GHz. Assim com o padrão 802.11n, este também suporta todos os padrões anteriores, outro ponto importante deste padrão é que existe um suporte para transmissões múltiplas de dados para clientes conectados, ou seja, se algum cliente estiver utilizando bastante recursos da rede sem fio, o normal seria a rede estar lenta para os outros clientes, porém com esse suporte este problema acaba.

A tabela 2 traz informações sobre as frequências utilizadas pelos padrões Wi-Fi citados a cima.

Tabela 2: Frequências utilizadas pelos padrões Wi-Fi

Padrões	Frequência (GHz)
802.11b	2,4
802.11a	5
802.11g	2,4 a 5
802.11i	5
802.11n	2,4 a 5
802.11ac	5

Fonte: O autor

2.2.3.2 802.15 (Bluetooth)

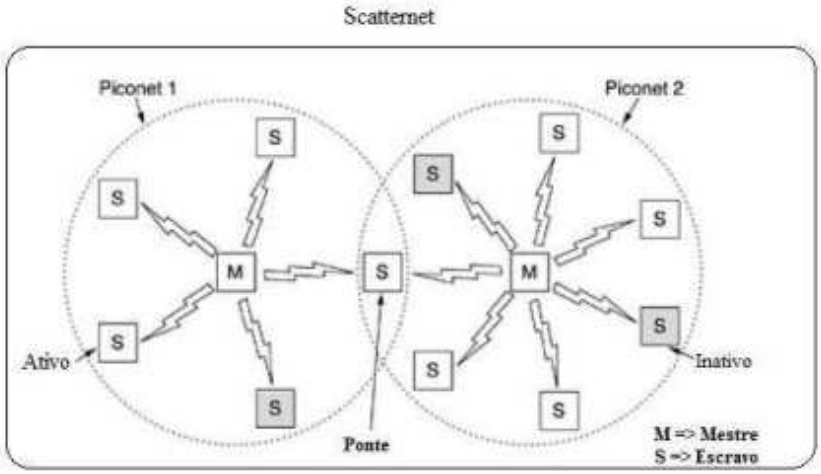
Segundo Forouzan (2008) e Tanenbaum (2011), originalmente o Bluetooth foi criado pela Ericsson Company e foi definido como uma rede WLAN, porém com o padrão 802.15 definido pela IEEE, o Bluetooth passou a ser uma rede da classificação WPAN.

De acordo com Rufino (2015), o Bluetooth foi desenvolvido para ser uma rede de custo reduzido, alcançando uma distância de 10 metros e assim como as primeiras tecnologias Wi-Fi, utiliza uma frequência de 2,4 GHz.

Forouzan (2008, p. 434), diz que “[...] uma rede Bluetooth é uma rede ad hoc, o que significa que é formada espontaneamente; os dispositivos, algumas vez chamados de *gadgets*, se localizam e criam uma rede chama piconet [...]”, ou seja, uma rede formada apenas por dispositivos conectados entre si, sem a necessidade de uma infraestrutura de rede com um ponto de acesso.

Tanenbaum (2011) e Forouzan (2008) afirmam que a arquitetura de uma rede Bluetooth é definida por piconets e scatternet, que pode ser vista na Figura 5.

Figura 5: Picontes e Scaternet



Fonte: Tanembaum (2011)

Conforme Forouzan (2008), Kurose e Ross (2014), Rufino (2015), uma piconet é uma rede onde existem até 8 dispositivos conectados, sendo um deles um dispositivo mestre ou primário e os demais, dispositivos escravos ou secundários.

A partir de um dispositivo secundário, pode-se fazer uma ponte para originar uma nova piconet e com isso se origina uma scatternet, que é um conjunto de piconets.

Assim como em redes do padrão 802.11 exigiu novas tecnologias devido aos avanços tecnológicos, as redes do padrão 802.15 também exigiram. O padrão mais utilizado e difundido atualmente é o 802.15.4, segundo IEEE 802.15.4 (2006) *apud* Steinhauser (2013, p. 3), “é um conjunto de especificações que tem como finalidade definir tanto o protocolo quanto o comportamento da comunicação entre dispositivos da rede”.

O mesmo autor complementa que este padrão trata apenas das camadas de níveis Físico (PHY) e de Enlace (MAC), na primeira camada são definidas as bandas de frequência e controle para economizar energia, e na segunda camada são definidas como é realizada a interface entre a camada PHY e a camada superior, que no caso é a camada de rede (NWK), entra outras tecnologias existentes para esta camada, existe uma conhecida como ZigBee.

Para Dantas (2010) *apud* Steinhauser (2013, p. 3):

> “A especificação ZigBee, foca nos protocolos de alto nível para dispositivos pequenos de rádio digital e com baixo consumo de energia, o que o torna tão

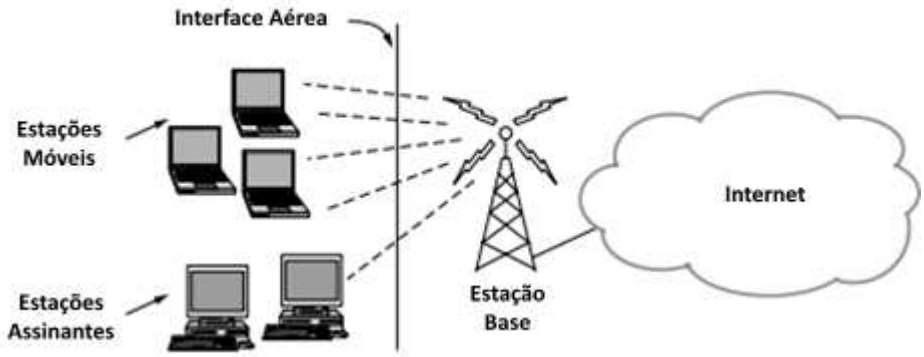
> atrativo para utilização em projetos que requeiram o mínimo de consumo de energia possível".

2.2.3.3 802.16 (WiMAX)

O padrão 802.16 surgiu através do problema de como as empresas fariam para que os cabos coaxiais, par trançado ou até mesmo cabos de fibra chegassem até milhões de residências sem ter um custo tão alto. Então as empresas chegaram à conclusão de que utilizar cabos seria inviável e de que as redes sem fio seria a melhor alternativa, com isso as empresas começaram a testar tecnologias desenvolvidas por elas mesmo sem um padrão a ser seguido e com isso ocorria vários problemas tanto por parte de *hardware* quanto *software* (TANEMBAUM, 2011).

A partir desta falta de padrão e problemas decorrentes, a IEEE formou um grupo para padronizar este tipo de rede WMAN e o número 802.16 foi definido como o padrão para a mesma. Este também é conhecido como WiMAX.

Figura 6: Arquitetura WiMax

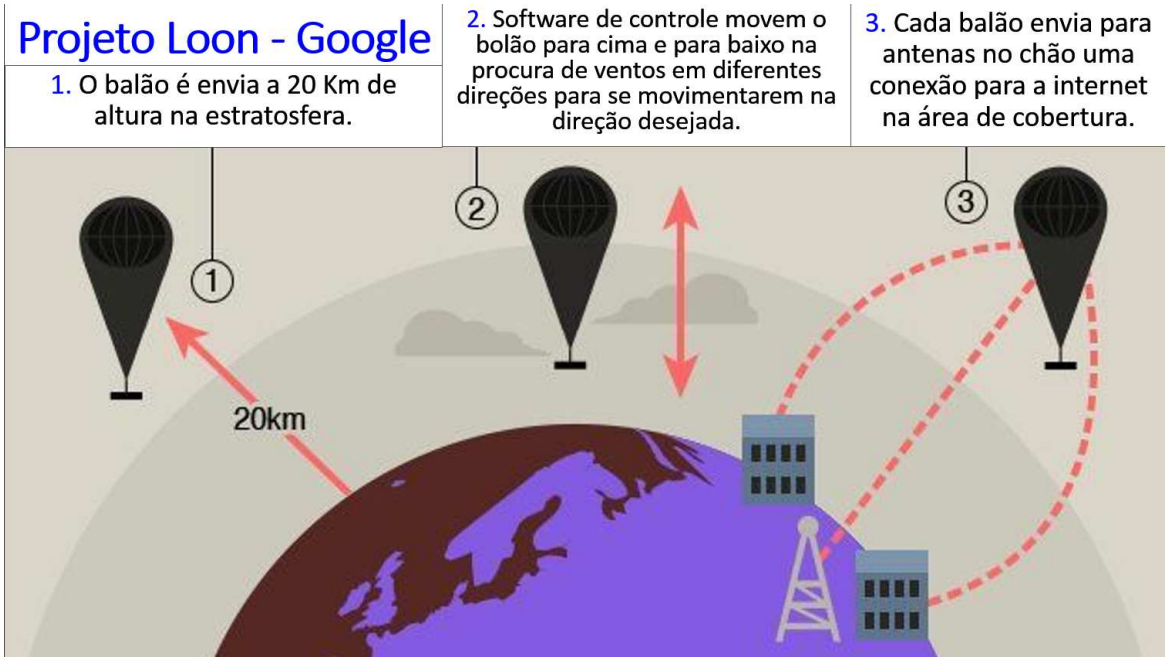


Fonte: adapatado de Tanembaum (2011)

Conforme a arquitetura do WiMAX apresentado na Figura 6, as estações bases conectam diretamente com os provedores e assim com a internet. Para realizar à comunicação entre as estações base e as estações é utilizado da tecnologia sem fio. Existem dois tipos de estações: estações assinantes, onde as mesmas têm uma localização fixa, por exemplo as casas; e estações móveis, onde as mesmas podem receber o serviço enquanto estão em movimentos, por exemplo dispositivos equipados com WiMAX (TANENMBAUM, 2011).

Entre as tecnologias mais recentes está o Projeto Loon da Google, o projeto teve seu início em 2013. Utiliza de tecnologias como o WiMax para fornecer Internet para pessoas em áreas rurais ou remotas, este utiliza de balões projetados como torres de sinais que possuem uma área de cobertura de 80 quilômetros de diâmetro no solo. Estes balões ficam na estratosfera a uma altitude de 20 quilômetros da superfície da Terra, como é mostrado na Figura 7.

Figura 7: Projeto Loon

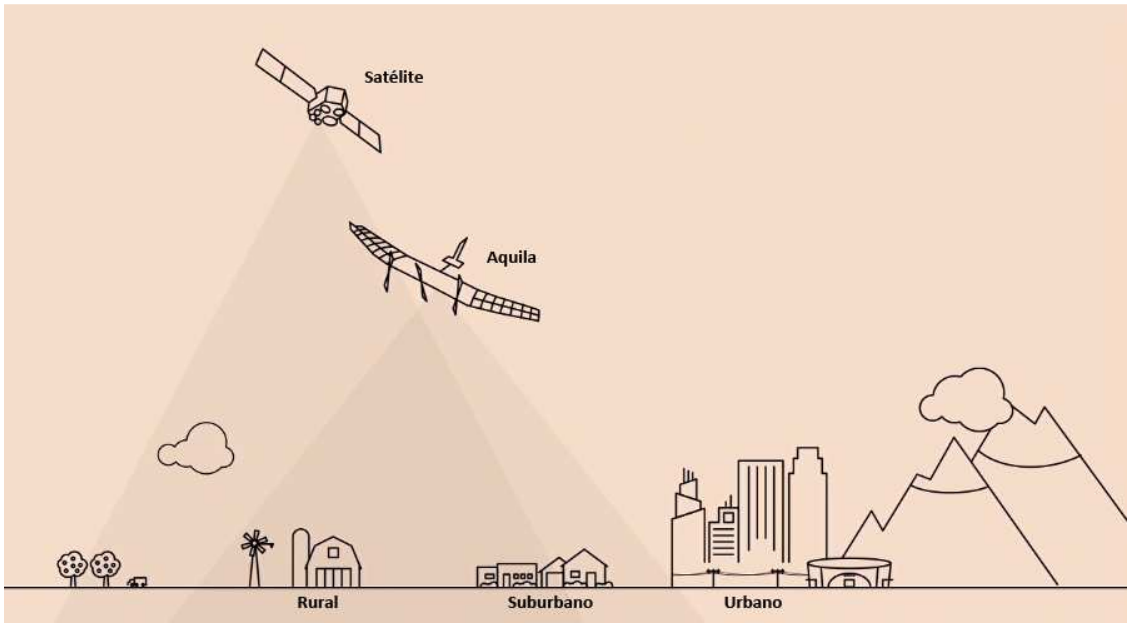


Fonte: Silveira (2015)[1]

Outra tecnologia é a Internet.org do Facebook, lançado em 2013 com o objetivo de fornecer acesso básico a Internet para o mundo todo. Esse projeto também utiliza da tecnologia WiMax, porém ao invés de balões como é mostrado no Projeto Loon, a Internet.org utiliza de aviões, conhecido como Aquila, não tripulados e de luz para transmissão de sinais para antenas que estão projetadas estrategicamente, como é mostrado na Figura 8.

[1] http://www.sanderlei.com.br/img/Noticia/Tecnologia/2015-11-11-06.png

Figura 8: Internet.org



Fonte: adaptado de Troyack (2015)[1]

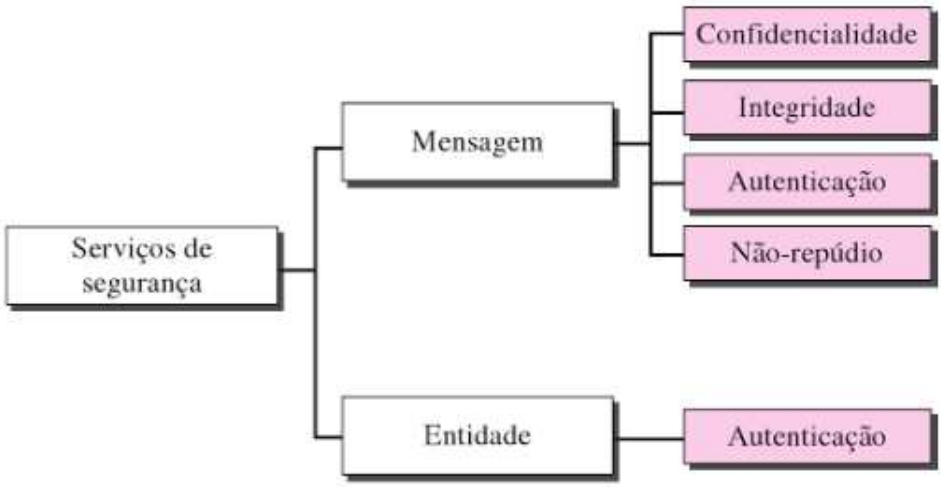
2.3 Segurança em Rede sem Fio

A segurança em rede tem como preocupação garantir que pessoas mal-intencionadas não consigam ler ou modificar mensagens enviadas a outros destinatários pela rede. Também se preocupa em garantir que pessoas não autorizadas não consigam acessar serviços remotamente. A maior parte dos problemas relacionadas à segurança de rede são causados por pessoas mal-intencionadas que tem como objetivo obter de algum benefício, chamar a atenção ou prejudicar alguém (TANENBAUM, 2011).

Furouzan (2008) aponta que, a segurança em uma rede de computadores pode ser dividida em cinco serviços, sendo quatro deles relacionadas as mensagens trocadas pela rede e último em relação a identificação de entidades, conforme a Figura 9.

[1] http://codigofonte.uol.com.br/noticias/facebook-e-internet-org-estao-construindo-drones-para-levar-internet-ate-lugares-remotos/.

Figura 9: Serviços de segurança



Fonte: Furouzan, 2008

Segundo o mesmo autor, a confidencialidade da mensagem significa que o emissor e receptor tem sigilo em relação a troca de dados realizada. A integridade da mensagem significa que os dados devem chegar ao receptor do mesmo modo que foi enviado pelo emissor. A autenticação da mensagem significa que o receptor precisa ter certeza de que o emissor é, de fato, quem diz ser. O não-repúdio da mensagem significa que o emissor não pode negar algo que realmente realizou. A autenticação de entidades significa que a entidade precisa de uma identificação válida para conseguir efetuar o acesso aos recursos da rede.

Tanenbaum (2011) também afirma sobre a divisão desses serviços, porém os trata como áreas interligadas nas quais os problemas de segurança das redes podem ser divididos.

2.3.1 Ameaças e vulnerabilidades a redes sem fio

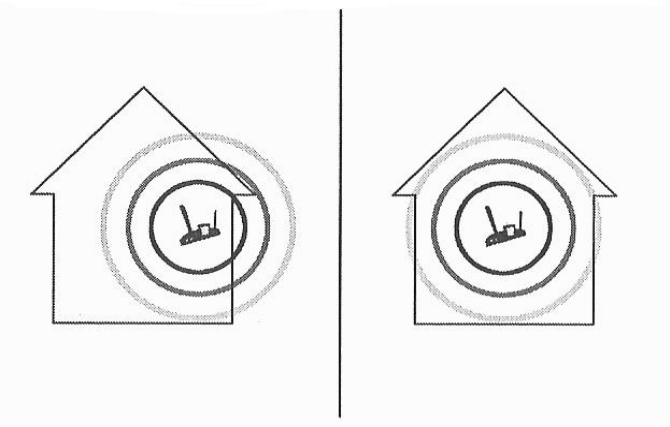
Shirey (2000) *apud* Stallings (2014), uma **ameaça** é o potencial para violação da segurança quando há uma circunstância, capacidade, ação ou evento que pode quebrar a segurança e causar danos. Ou seja, uma ameaça é um possível perigo que pode explorar uma vulnerabilidade.

Uma **vulnerabilidade** é uma falha ou fraqueza em um projeto, implementação ou operação e gerenciamento de um sistema que pode ser explorado para violar a política de segurança do sistema. Essa vulnerabilidade pode ser explorada por uma ameaça e consequentemente pode ser atacada (SHIREY, 2000).

Para Rufino (2014), assim como as redes cabeadas, as redes sem fio estão sujeitas a ameaças e vulnerabilidades, entre as mais comuns estão as apresentadas abaixo. Sendo elas:

Um dos primeiros problemas, é a questão da **segurança física**, nela os administradores de redes se preocupam mais com a parte lógica do que a parte física de uma rede sem fio, em relação a rede cabeada existem diversos tipos de fatores que possam impedir a entrada de um possível atacante como portaria, credenciais, etc., mas em uma rede sem fio esse fator muda, pelo simples de fato de que o sinal se propaga pelo ar, então o atacante não precisa estar necessariamente no local para realizar um possível ataque, como mostra a Figura 10.

Figura 10: Posição física de um AP



Fonte: Rufino (2014)

Então, no momento da implementação de uma rede sem fio deve-se levar em consideração a potência do sinal do transmissor que está utilizando, também não se deve desconsiderar o fato de que este deva estar em um local seguro sem acesso a qualquer um.

Os equipamentos transmissores de rede sem fio, como um roteador, vêm por padrão de **configuração de fábrica** com mecanismos de segurança desabilitados, devido ao fato da facilidade de instalação, incompatibilidade com dispositivos, etc. Isso acarreta em alvos fáceis para possíveis ataques.

Além dos mecanismos de segurança desabilitados, os equipamentos também vêm com usuário e senha padrão para acesso nas configurações dos mesmos. Se um atacante conseguir acesso à rede e o endereço do dispositivo, este pode se tornar um alvo fácil de ataques.

Outro ponto importante na segurança de um equipamento, são os protocolos que estão habilitados, por exemplo o SNMP, que [...]”é responsável por prover informações gerenciais sobre o equipamento e tráfego”[...], se este estiver habilitado e acessível ao atacante, ele consegue diversas informações da sua rede, bem como dispositivos conectados.

As redes sem fios estão expostas a serem alvos de um **mapeamento do ambiente** pelos atacantes, esse mapeamento tem como objetivo mapear o ambiente coletando informações sobre a rede, com isso o atacante consegue realizar um melhor ataque.

Existem dois tipos de mapeamentos: o passivo, onde o atacante consegue realizar a varredura sem estar conectado na rede para não ser detectado por algum mecanismo de segurança através de ferramentas; e o ativo, onde o atacante consegue identificar os equipamentos em operação, com isso é possível identificar vulnerabilidades conhecidas nesses equipamentos já que tem o conhecimento do endereço MAC e eles são ligados a fabricantes.

Como as redes sem fio utilizam de ondas de radiofrequência para propagar o sinal pelo ar, é possível realizar a **captura de tráfego** das mesmas através de equipamentos, como *notebooks* e ferramentas de captura. Com isso em mãos, o atacante pode realizar uma análise nos pacotes capturados através das ondas de radiofrequência para roubo de informações.

Um atacante tem diversas razões para acessar uma rede sem fio, entre as principais estão testes, saída para internet e furto de informações. Para acessar uma rede sem fio, o atacante depende do **modo que o equipamento está configurado**, existem dois tipos de configurações: a aberta, onde o SSID é fornecido pelo equipamento, podendo ou não exigir uma senha para realizar o acesso e também para acessar a página de configuração; e a fechada, onde o SSID não é disponibilizado pelo equipamento. Mesmo em uma configuração fechada é possível descobrir o SSID através de ferramentas de captura de tráfego.

Muitos administradores de redes ligam **redes sem fio em redes cabeadas** e esquecem dos mecanismos de segurança pelo fato de que creem que a segurança que está configurada para a rede cabeada é o suficiente. Se um atacante decidir atacar a essa rede sem fio, ele conseguirá acesso a tudo que trafega na mesma, inclusive na rede cabeada.

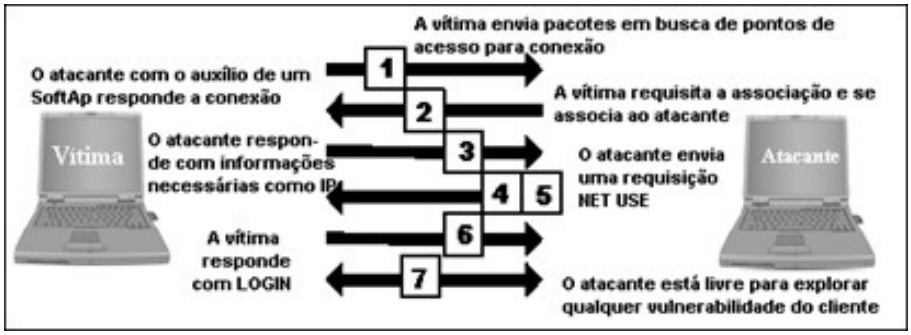
2.3.2 Ataques a redes sem fio

Segundo RFC 2828 (2000), um **ataque** é um ataque à segurança do sistema, derivado de uma ameaça inteligente, ou seja, um ato inteligente que é uma tentativa deliberada (especialmente no sentido de um método ou técnica) de burlar os serviços de segurança e violar a política de segurança de um sistema.

Para Cutrim (2013), os ataques a rede sem fio têm como objetivo obter informações sem autorização, acesso indevido e ataques de negação de serviço. Entre os diversos tipos de ataque, os mais comuns e que mais tem destaque são sete tipos. Sendo eles:

O primeiro tipo é ***Access Point Spoofing*** (Associação Maliciosa), ocorre por meio de um computador malicioso usado como um ponto de acesso de rede sem fio na qual a vítima tenta acessar e esse computador gera as informações necessárias para que ela tenha acesso e a partir desse ponto qualquer informação vulnerável da vítima está sendo exposta, conforme é apresentado na Figura 11.

Figura 11: AP *Spoofing*

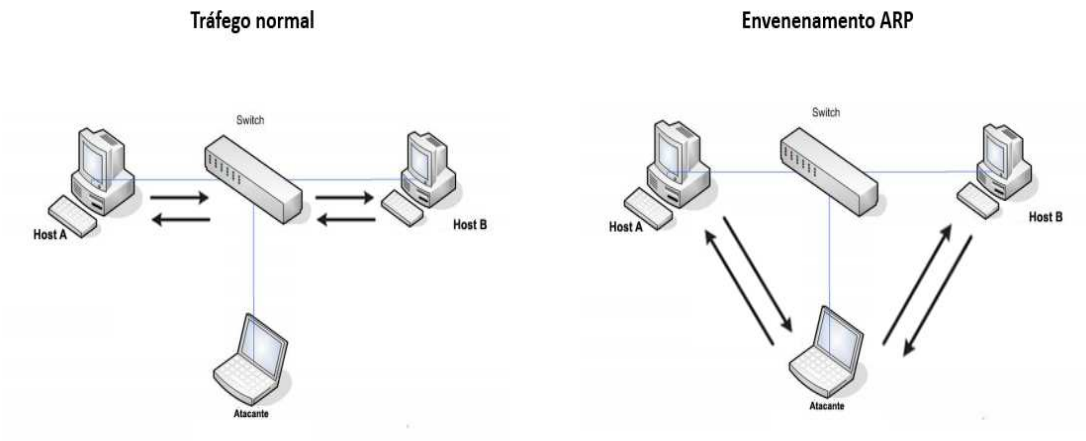


Fonte: Seruffo (2010)[1]

O segundo tipo é **Envenenamento ARP**, ele ocorre quando a vítima está conectada na mesma rede do atacante. Este tipo de ataque, pode por meio da rede sem fio chegar a rede cabeada e com isso não somente as informações dos usuários ficam expostas e sim as informações de todo local até da rede interna, conforme a Figura 12.

[1] http://slideplayer.com.br/slide/5625405/

Figura 12: Envenenamento ARP



Fonte: O autor

Tudo que passa entre os hosts A e B está passando pelo Atacante e deixa as informações expostas para o mesmo.

O terceiro tipo é **MAC *Spoofing***, ocorre por meio do endereço físico do dispositivo mais conhecido como MAC, as redes que só podem ser acessadas por MACs autorizados, por meio de algum software específico, o atacante consegue obter um desses e alterar o de sua máquina obtendo acesso à rede, como mostra a Figura 13.

Figura 13: MAC *Spoofing*

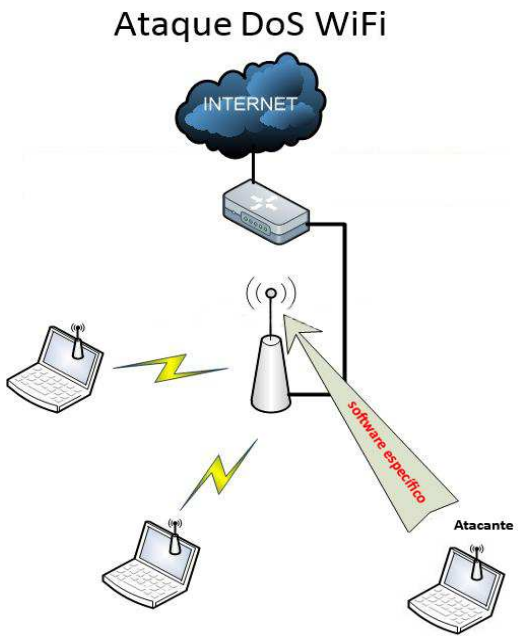
```
#ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:02:2D:3D:4F:3C
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:13 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:1623 (1.5 Kb)  TX bytes:0 (0.0 b)
          Interrupt:3 Base address:0x100

#ifconfig eth0 down
#ifconfig eth0 hw ether 1B:11:CE:DC:CE:00
#ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 1B:11:CE:DC:CE:00
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:14 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:1659 (1.6 Kb)  TX bytes:0 (0.0 b)
          Interrupt:3 Base address:0x100
```

Fonte: Duarte (2003)[1]

[1] http://smeduquedecaxias.rj.gov.br/nead/Biblioteca/Forma%C3%A7%C3%A3o%20Continuada/Tecnologia/cursos/seguranca/ataques%20e%20vulnerabilidades%20em%20redes%20sem%20fio.pdf

O quarto tipo é **Negação de serviço** (*Denial of Service* – DoS), ocorre quando o atacante por meio de softwares específicos que utilizam da radiofrequência para emitir sinais para uma rede sem fio e faz com que os usuários conectados fiquem se desconectando e assim não podem ficar muito tempo na mesma, como é mostrado na Figura 14.

Figura 14: Ataque DoS



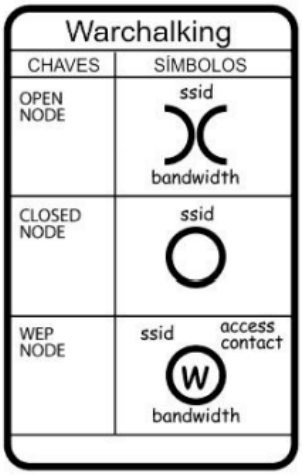
Fonte: O autor

O quinto tipo é **WLAN *Scanner*** (Ataques de Vigilância), ocorre por meio de software e equipamentos específicos para descobrir onde estão localizados os aparelhos.

O sexto tipo é ***Wardriving***, ocorre por meio de que o atacante percorra um determinado local descobrindo por meio visual a localidade dos aparelhos de redes sem fio para que que possam ser invadidos ou ter suas configurações restauradas ou até mesmo para serem roubados

O último tipo é ***Warchalking***, ocorre pelo *Wardriving* só que os atacantes por meio de algum recurso de pichação marcam esses determinados locais com símbolos específicos para que outros atacantes tenham noção de que existe uma rede e qual seu tipo naquele local, conforme a Figura 15.

Figura 15: simbologia warchalking



Fonte: Projetos de Redes (2012) *apud* Moretti e Bellezzi (2014)[1]

De acordo com Lucchese (2007) *apud* Moretti e Bellezi (2014), o primeiro símbolo se refere a uma rede sem fio sem senha, o segundo se refere a uma rede sem fio com senha e o último a uma rede sem fio com senha e que utiliza do método criptográfico WEP.

2.3.3 Técnicas seguras

Uma das principais técnicas seguras utilizadas em uma rede de computadores é a utilização da **criptografia.** CERT (2012) afirma que:

> "A criptografia, considerada como a ciência e a arte de escrever mensagens em forma cifrada ou em código, é um dos principais mecanismos de segurança que você ê pode usar para se proteger dos riscos associados ao uso da Internet".

O mesmo autor, também afirma que por meio da criptografia é possível proteger os dados sigilosos que estão armazenados no seu dispositivo, criar áreas específicas em seu computador com criptografia para que todo dado armazenado seja criptografado automaticamente, proteção de *backups* contra acessos não autorizados e proteção de comunicações realizadas pela Internet.

De acordo com Kurose e Ross (2014, p. 497 e 498), "as técnicas criptográficas permitem que um remetente disfarce os dados de modo que um intruso não consiga

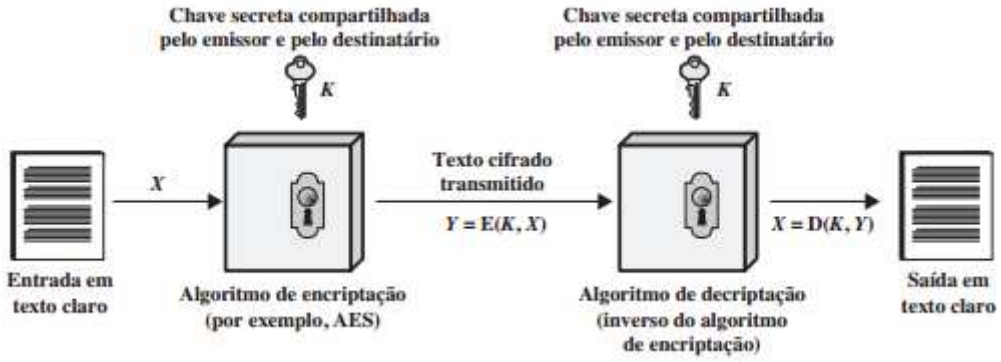
[1] http://revistatis.dc.ufscar.br/index.php/revista/article/view/73/67

obter nenhuma informação dos dados interceptados” e que o destinatário consiga recuperar os dados originais a partir dos dados disfarçados.

Dependendo do tipo de chave utilizada, os métodos criptográficos podem ser divididos em criptografia de chave simétrica e criptografia de chaves assimétricas (CERT, 2012).

Stallings (2014) e CERT (2012) apontam que, a **criptografia de chave simétrica,** também chamada de encriptação convencional ou encriptação de chave única, utiliza de uma mesma chave para emissor e destinatário tanto para encriptação quanto para decriptação, como é apresentado na Figura 16.

Figura 16: Criptografia de chave simétrica

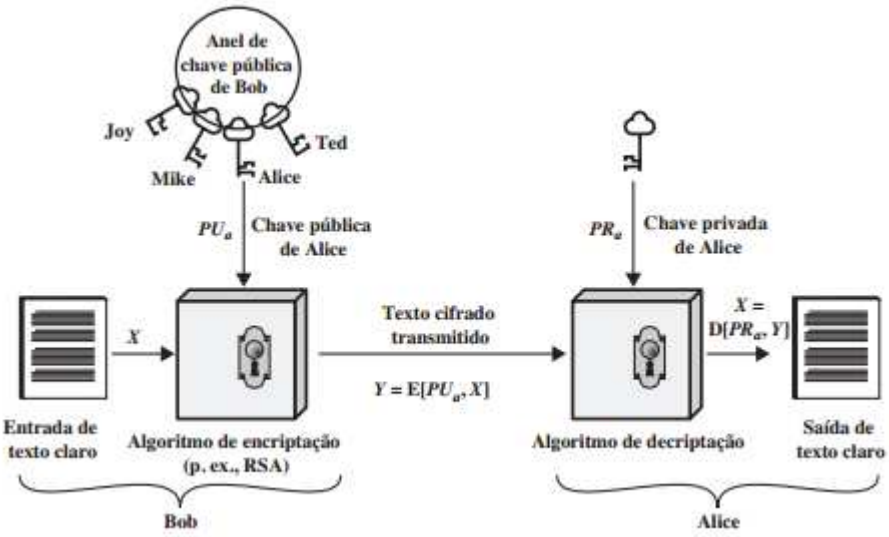


Fonte: Stallings (2014)

Para Stallings (2014), a **criptografia de chaves assimétricas**, também conhecida como criptografia de chave pública, utiliza de duas chaves, uma pública e uma privada, sendo que uma delas é utilizada para encriptação e a outra para decriptação.

O mesmo autor afirma que, cada usuário gera um par de chaves e torna uma delas visível para outros usuários, chave pública, e a outra mantém em segredo, chave privada. Se Bob deseja enviar uma mensagem secreta para Alice, ele utiliza a chave pública dela para encriptar e somente Alice conseguirá decriptar com sua chave privada, como mostra a Figura 17.

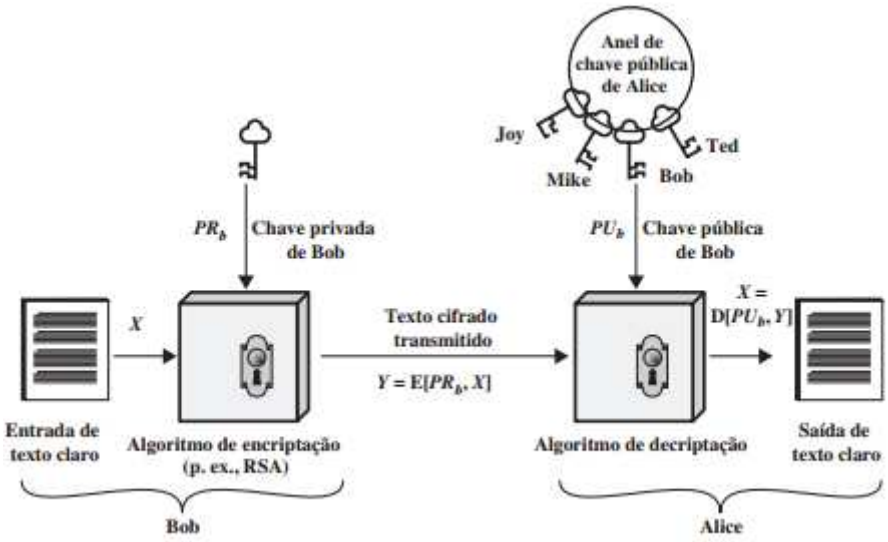
Figura 17: encriptação assimétrica com chave pública



Fonte: Stallings (2014)

Se Bob deseja enviar uma mensagem para todos que conhecem sua chave pública, inclusive Alice, ele encripta utilizando sua chave privada, como mostra a Figura 18.

Figura 18: encriptação assimétrica com chave privada



Fonte: Stallings (2014)

Segundo Choi (2008) *apud* Stallings (2014), os **métodos criptográficos utilizados em uma rede sem fio** têm como objetivo a proteção do AP e transmissões

wireless. Os protocolos criptográficos utilizados são três tipos sendo WEP, WPA e WPA2.

O algoritmo WEP, opera na camada de enlace no do modelo de referência ISO/OSI utilizando o método criptográfico Roteamento Coloniale 4 (RC4) da empresa RSA Data Security, Inc.

Ele é um algoritmo de chave pública que usa um vetor de inicialização de 24 bits e uma chave secreta compartilhada de 40 ou 104 bits, essa chave concatenada com o vetor de inicialização formam uma chave de 64 ou 128 bits que é utilizada para criptografar as informações.

Para manter a integridade da informação criptografada, o WEP utiliza da Checagem de Redundância (CRC-32) para calcular a Soma de Verificação (checksum) na informação enviada, então após o receptor receber a informação, o checksum é recalculado garantindo a integridade. No padrão 802.11 é utilizado a chave de 128 bits.

A principal desvantagem desse algoritmo é que um usuário mal-intencionado com a ajuda de algum meio de escuta na rede, pode obter a chave tornando possível a decriptação dos dados.

O algoritmo WPA, foi desenvolvido para resolver os problemas decorrentes no algoritmo de criptografia WEP. Ele foi criado em conjunto com da Wi-Fi Alliance com o IEEE com o objetivo de fornecer um tratamento mais seguro e ao mesmo tempo compatível com o hardware utilizado pelo WEP.

Para realizar a criptografia das informações o WPA utiliza do protocolo Temporal Key Integrity Protocol (TKIP) e também de uma chave previamente compartilhada (*pre-shared key* ou WPA-PSK).

O algoritmo WPA2**,** segundo CISCO (2016), utiliza do método criptográfico Advanced Encryption Standard (AES), diferente do TKIP utilizado pelo WPA que gera uma chave temporária, o AES gera uma nova chave a cada sessão específica a cada cliente que for conectado.

Outra técnica segura para redes sem fio, mais utilizada em redes públicas, é conhecida como **isolamento AP**. De acordo com Lynksys ([s.d]), essa técnica faz com que os dispositivos conectados em uma rede sem fio apenas consigam realizar a comunicação com o AP, mas não com outros, ou seja, é criado redes virtuais para cada dispositivo que esteja conectado e partir disso o mesmo não consegue usar ou compartilhar recursos com outros. Esta técnica permite com o que o atacante não

consiga conhecer os nós participantes da rede e possivelmente realizar varreduras com intenção de roubar dados dos demais dispositivos que estão conectados na mesma rede.

Uma técnica voltada para os usuários, é o uso ***firewall* pessoal**, que segundo CERT (2012), protege o dispositivo pessoal, seja ele um computador ou dispositivo móvel, contra acessos não autorizados. Além disso, também pode evitar tentativas de exploração de vulnerabilidades e coleta de informações por pessoas mal-intencionadas.

3 METODOLOGIA DA PESQUISA

Foi realizado uma pesquisa de campo nas redes sem fio de quatro locais, sendo um ambiente acadêmico, um ambiente público, um ambiente comercial e um ambiente de saúde.

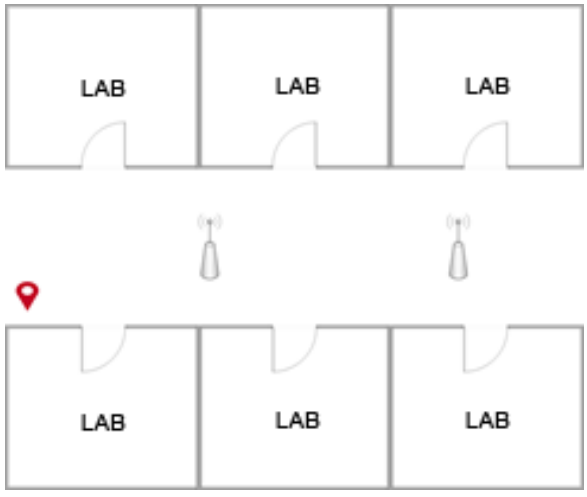
O objetivo de se realizar esta pesquisa de campo foi constatar o quão seguro ou inseguro são as redes sem fio utilizadas pelas pessoas no dia-a-dia para acessar a Internet nestes locais e que estas, na maioria das vezes, não têm nenhum conhecimento sobre os riscos que correm estando conectados nestas redes.

3.1 Descrição dos Cenários

Como citado anteriormente, os cenários se constituíram da rede sem fio de quatros locais, estes apresentados por imagens meramente ilustrativas, onde o ponto vermelho indica o local de onde o teste foi realizado.

O primeiro cenário foi um ambiente acadêmico (uma faculdade), os testes foram realizados em um corredor onde continham os laboratórios de informática e os APs conforme a Figura 19. Este foi escolhido para mostrar que mesmo em um ambiente onde a rede sem fio era para ser segura, existem diversas ameaças e riscos que um usuário pode correr estando conectado na mesma.

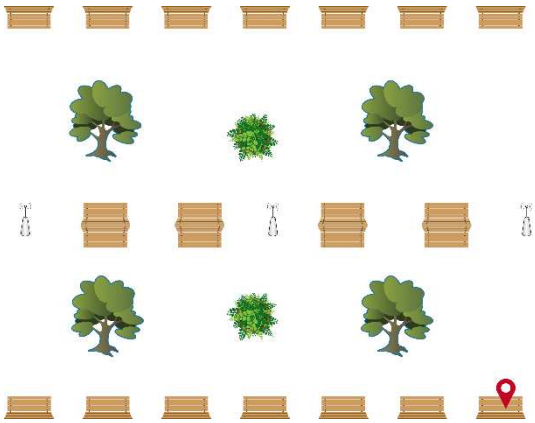
Figura 19: Ambiente acadêmico



Fonte: O autor

O segundo cenário foi um ambiente público (uma praça pública), os testes foram realizados em um banco, conforme a Figura 20. Este foi escolhido para as pessoas se questionarem se devem ou ser conectar a redes sem fio que qualquer pessoa pode ter acesso, e também mostrar as ameaças e riscos que podem correr.

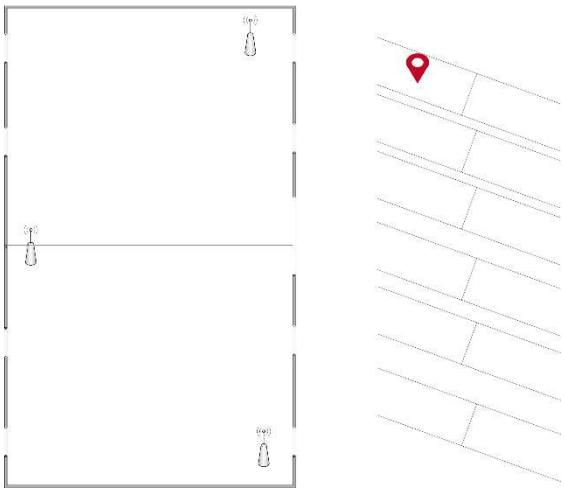
Figura 20: Ambiente público



Fonte: O autor

O terceiro cenário foi um ambiente comercial (um shopping), os testes foram realizados em um estacionamento, conforme a Figura 21. Este foi escolhido com a intenção de mostrar os riscos e ameaças que os usuários podem correr estando conectados à rede sem fio de bares, lojas, shopping, entre outros diversos ambientes comerciais.

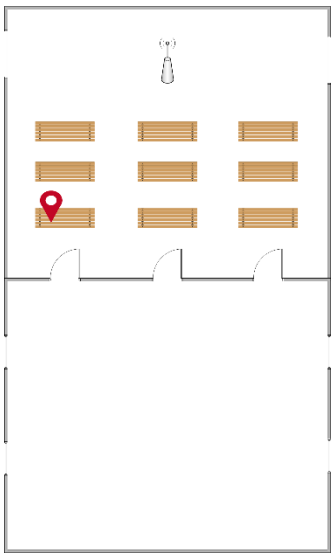
Figura 21: Ambiente comercial



Fonte: O autor

O quarto cenário foi um ambiente de saúde (um hospital), os testes foram realizados em uma sala de espera, conforme a Figura 22. Este foi escolhido para mostrar que mesmo em ambientes como um posto de saúde ou hospital, os usuários podem correr riscos e ameaças.

Figura 22: Ambiente de Saúde



Fonte: O autor

3.2 Testes

Os testes realizados se constituíram em quatro, sendo eles do tipo de ataque WLAN *Scanner*, explorando as ameaças e vulnerabilidades citadas anteriormente na seção 2.3.1.

Teste 1 – com smartphone

O primeiro teste foi realizado a partir de um aplicativo de *smartphone* com o objetivo de identificar os nós participantes da rede. Este aplicativo é o Fing, que tem como objetivo descobrir todos dispositivos conectados na rede apresentando a marca e fabricante, isto inclui computadores, *notebooks*, *smartphones*, roteadores, switches, servidores, etc., também pode realizar a varredura de serviços abertos.

No ambiente acadêmico estes testes trouxeram os seguintes resultados, conforme as Figuras 23 e 24.

Figura 23: Identificação de nós no ambiente Acadêmico

Fonte: O autor

Figura 24: Serviços no ambiente acadêmico

Fonte: O autor

No ambiente público foi possível obter os seguintes resultados, conforme as Figuras 25 e 26.

Figura 25: Identificação de nós no ambiente público

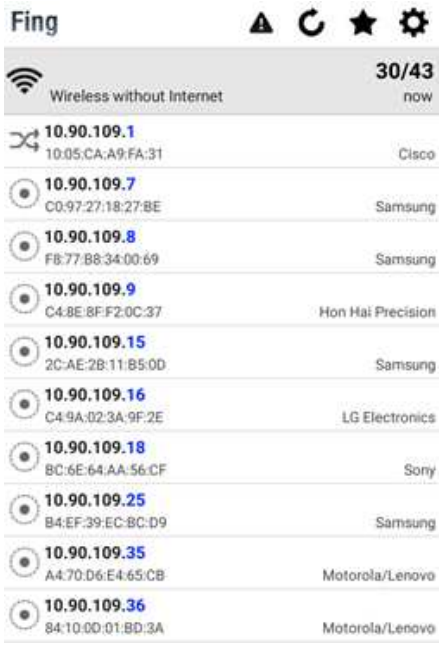
Fonte: O autor

Figura 26: Serviços no ambiente público

Fonte: O autor

No ambiente comercial foi possível obter os seguintes resultados, conforme as Figuras 27 e 28.

Figura 27: Identificação de nós no ambiente comercial



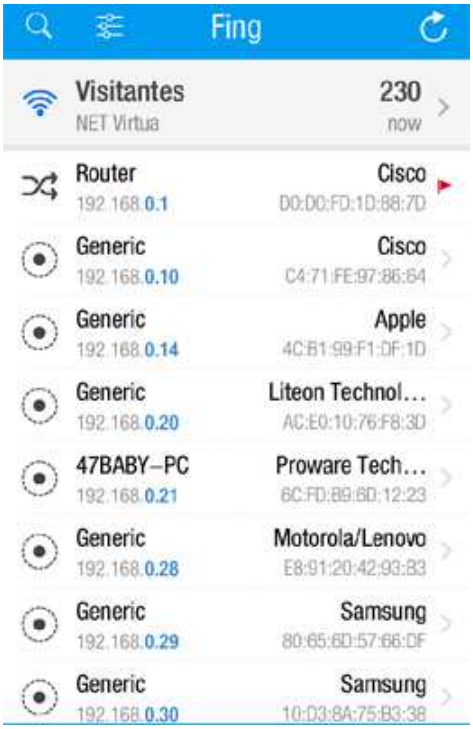
Fonte: O autor

Figura 28: Serviços no ambiente comercial

Fonte: O autor

No ambiente de saúde foi possível obter os seguintes resultados, conforme as Figuras 29 e 30.

Figura 29: Identificação de nós no ambiente de saúde



Fonte: O autor

Figura 30: Serviços no ambiente de saúde

Fonte: O autor

Teste 2 – com Wireshark

Por meio do segundo teste, foi possível capturar os pacotes que estavam circulando pela rede, a partir disto é possível filtrar pacotes com vulnerabilidades conhecidas e realizando a leitura deste pode-se encontrar senhas.

O segundo teste foi realizado a partir do *software* Wireshark com o objetivo de capturar pacotes que estavam trafegando na rede sem fio. Este software é um dos mais famosos entre os que analisam tráfego de rede.

Nos ambientes acadêmico, comercial e de saúde foram possíveis realizar esta captura, conforme as Figuras 31, 32 e 34. Porém no ambiente público, devido a técnica de isolamento AP, somente foi possível capturar os pacotes do próprio dispositivo de onde estava sendo realizado o teste, conforme a Figura 33.

Figura 31: Captura de pacotes no ambiente acadêmico

704	37.946917461	Tecnomen_30:38:90	Broadcast	ARP	60 Who has 192.168.100.254? Tell 192.168.102.239
705	38.047046981	Tecnomen_30:38:90	Broadcast	ARP	60 Who has 192.168.100.254? Tell 192.168.102.184
706	38.149521875	Azurewav_f6:67:96	Broadcast	ARP	60 Who has 192.168.100.254? Tell 192.168.101.12
707	38.181586392	Tp-LinkT_28:27:bd	Broadcast	ARP	42 Who has 192.168.100.122? Tell 192.168.103.202
708	38.181628315	Tp-LinkT_28:27:bd	Broadcast	ARP	42 Who has 192.168.100.125? Tell 192.168.103.202
709	38.181659237	Tp-LinkT_28:27:bd	Broadcast	ARP	42 Who has 192.168.100.178? Tell 192.168.103.202
710	38.181664360	Tp-LinkT_28:27:bd	Broadcast	ARP	42 Who has 192.168.100.197? Tell 192.168.103.202
711	38.181668216	Tp-LinkT_28:27:bd	Broadcast	ARP	42 Who has 192.168.100.53? Tell 192.168.103.202
712	38.249633952	Tp-LinkT_28:27:bd	Broadcast	ARP	42 Who has 192.168.100.254? Tell 192.168.103.202

Fonte: O autor

Figura 32: Captura de pacotes no ambiente comercial

22	9.720316976	Motorola_34:7a:10	Broadcast	ARP	60 Who has 10.90.109.2? Tell 10.90.109.81
23	9.720464948	Motorola_34:7a:10	Broadcast	ARP	60 Who has 10.90.109.3? Tell 10.90.109.81
24	9.721665043	Motorola_34:7a:10	Broadcast	ARP	60 Who has 10.90.109.4? Tell 10.90.109.81
25	9.724975324	Motorola_34:7a:10	Broadcast	ARP	60 Who has 10.90.109.5? Tell 10.90.109.81
26	9.762986368	Motorola_34:7a:10	Broadcast	ARP	60 Who has 10.90.109.6? Tell 10.90.109.81
27	9.763090342	Motorola_34:7a:10	Broadcast	ARP	60 Who has 10.90.109.7? Tell 10.90.109.81
28	9.763277826	Motorola_34:7a:10	Broadcast	ARP	60 Who has 10.90.109.8? Tell 10.90.109.81
29	9.763396228	Motorola_34:7a:10	Broadcast	ARP	60 Who has 10.90.109.9? Tell 10.90.109.81
30	9.763649986	Motorola_34:7a:10	Broadcast	ARP	60 Who has 10.90.109.10? Tell 10.90.109.81

Fonte: O autor

Figura 33: Captura de pacotes no ambiente público

10	38.070012032	Routerbo_e8:c4:31	Broadcast	ARP	60 Who has 192.168.12.5? Tell 192.168.12.1
11	39.402070069	Routerbo_e8:c4:31	Broadcast	ARP	60 Who has 192.168.12.233? Tell 192.168.12.1
12	40.435438528	Routerbo_e8:c4:31	Broadcast	ARP	60 Who has 192.168.12.200? Tell 192.168.12.1
13	45.238069465	Routerbo_e8:c4:31	Broadcast	ARP	60 Who has 192.168.12.5? Tell 192.168.12.1
14	46.468324262	Routerbo_e8:c4:31	Broadcast	ARP	60 Who has 192.168.12.5? Tell 192.168.12.1
15	47.388535173	Routerbo_e8:c4:31	Broadcast	ARP	60 Who has 192.168.12.233? Tell 192.168.12.1
16	48.108304877	Routerbo_e8:c4:31	Broadcast	ARP	60 Who has 192.168.12.200? Tell 192.168.12.1
17	49.231798060	Routerbo_e8:c4:31	Broadcast	ARP	60 Who has 192.168.12.200? Tell 192.168.12.1
18	49.231953770	Routerbo_e8:c4:31	Broadcast	ARP	60 Who has 192.168.12.5? Tell 192.168.12.1

Fonte: O autor

Figura 34: Captura de pacotes no ambiente de saúde

3	5.237652	HonHaiPr_a2:a6:e3	Broadcast	ARP	42 Who has 192.168.0.1? Tell 192.168.1.30
22	15.300638	HonHaiPr_a2:a6:e3	Broadcast	ARP	42 Who has 192.168.0.1? Tell 192.168.1.30
30	25.361319	HonHaiPr_a2:a6:e3	Broadcast	ARP	42 Who has 192.168.0.1? Tell 192.168.1.30
37	35.427727	HonHaiPr_a2:a6:e3	Broadcast	ARP	42 Who has 192.168.0.1? Tell 192.168.1.30
51	45.499623	HonHaiPr_a2:a6:e3	Broadcast	ARP	42 Who has 192.168.0.1? Tell 192.168.1.30
60	55.657896	HonHaiPr_a2:a6:e3	Broadcast	ARP	42 Who has 192.168.0.1? Tell 192.168.1.30
64	65.725309	HonHaiPr_a2:a6:e3	Broadcast	ARP	42 Who has 192.168.0.1? Tell 192.168.1.30
92	75.780662	HonHaiPr_a2:a6:e3	Broadcast	ARP	42 Who has 192.168.0.1? Tell 192.168.1.30
265	85.852690	HonHaiPr_a2:a6:e3	Broadcast	ARP	42 Who has 192.168.0.1? Tell 192.168.1.30

Fonte: O autor

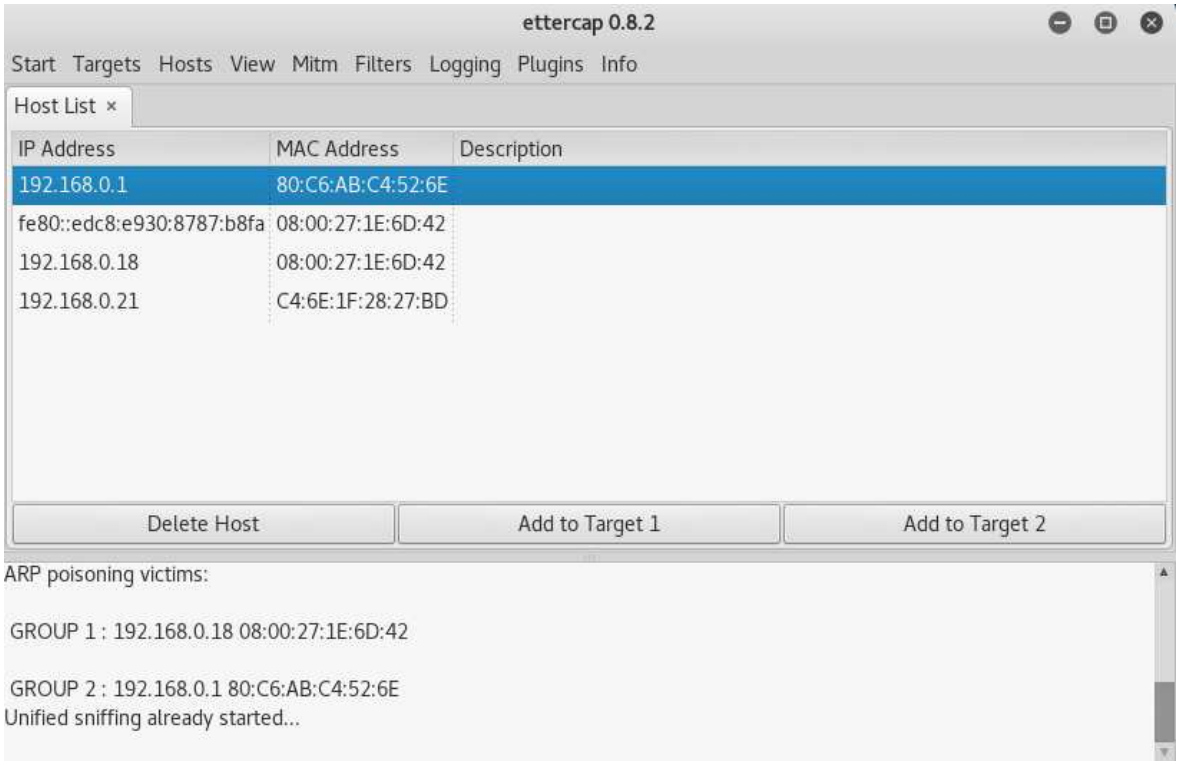
Nas redes que foram possíveis capturar os pacotes de todos dispositivos, é possível filtrar quais deles estão navegando pela Internet utilizando o protocolo HTTP

ou HTTPS. A partir disto, é possível explorar uma vulnerabilidade em um protocolo de segurança utilizado pelo mesmo, conhecido como SSL que de acordo com CERT (2012), utiliza métodos criptográficos para “assegurar a confidencialidade e integridade das informações”.

Por questões éticas e também a lei 12.737/2012, conhecida como Lei Carolina Dieckmann, que segundo BRASIL (2012), “dispõe sobre a tipificação criminal de delitos informáticos”, esta exploração foi feita por meio de um experimento em um ambiente virtual próprio e controlado.

Este teste consistiu em identificar quais *hosts* estavam utilizando do protocolo HTTP e HTTPS por meio do Wireshark e definir um destes *hosts* e o gateway padrão como alvo, utilizando o *software* Ettercap, que utiliza do ataque Envenenamento ARP, citado na seção 2.3.2, conforme a Figura 35.

Figura 35: Seleção de alvos no Ettercap



Fonte: O autor

Com o *host* 192.168.0.18 e o gateway padrão 192.168.0.1 selecionados como alvos, foi realizado um redirecionamento de portas através do IPTABLES, que é uma ferramenta para criação e gerenciamento de *firewalls*, onde a porta 80 (HTTP) foi redirecionada para a porta 15000 (porta livre) para que todo tráfego HTTP da rede

passasse antes pelo dispositivo de onde estava sendo realizado o teste para depois ir para o roteador, conforme a Figura 36.

Figura 36: Redirecionamento de porta IPTABLES

```
root@kali:~# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIR
ECT --to-port 15000
```

Fonte: O autor

Após isto, foi executado o *software* SSLSTRIP, que “estripa” o protocolo HTTPS a fim de identificar usuários e senhas no protocolo SSL, com os parâmetros “-l” para identificar a porta e “-f” para forçar a captura de requisições seguras, conforme a Figura 37.

Figura 37: Execução do SSLSTRIP

```
root@kali:~# sslstrip -l 15000 -f

sslstrip 0.9 by Moxie Marlinspike running...
```

Fonte: O autor

Em uma máquina virtual utilizando os navegadores Internet Explorer 8, Mozilla Firefox e Edge, foram acessados aos *sites* Facebook, Outlook, BOL Mail, UOL Mail, Office 365 e Yahoo, por meio de contas de usuários inexistentes.

Através do navegador Internet Explorer 8, foi possível capturar as senhas de todos *sites* acessados, exceto no *site* Yahoo que realiza uma autenticação em duas etapas, sendo necessário um usuário existente para depois o uso de senha, conforme a Figura 38.

Figura 38: Usuários e senhas no Internet Explorer 8

```
HTTP : 31.13.85.36:80 -> USER: hugo_teste123@facebook.com  PASS: teste123  INFO: http://www.facebook.com/

HTTP : 131.253.61.98:80 -> USER: hugo_teste123@outlook.com  PASS: teste123  INFO: http://login.live.com/login.srf?
wa=wsignin1.0&ct=1477678656&rver=6.6.6556.0&wp=MBI_SSL&wreply=https://outlook.live.com/owa/
&id=292841&CBCXT=out&cobra

HTTP : 186.234.131.130:80 -> USER: hugo_teste123  PASS: teste123  INFO: http://email.bol.uol.com.br/login

HTTP : 104.41.13.126:80 -> USER: hugo_teste123@hotmail.com  PASS: teste123  INFO: http://login.microsoftonline.com/??
mkt=pt-BR

HTTP : 98.139.21.169:80 -> USER: hugo_teste123@yahoo.com.br  PASS:   INFO: http://
login.yahoo.com/?.src=ym&.intl=br&.lang=pt-BR&.done=https://mail.yahoo.com
```

Fonte: O autor

Já no Mozilla Firefox, por ser um navegador com mais segurança e mais atualizado, foi apenas possível capturar as senhas dos *sites* BOL Mail e UOL Mail, conforme a Figura 39.

Figura 39: Usuários e senhas no Mozilla Firefox

```
HTTP : 186.234.131.130:80 -> USER: hugo_teste123  PASS: teste123  INFO: http://email.bol.uol.com.br/login/
HTTP : 186.234.3.128:80 -> USER: hugo_teste123  PASS: teste123  INFO: http://email.uol.com.br/login
```

Fonte: O autor

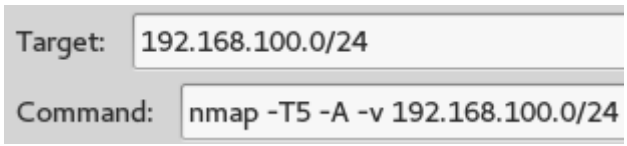
No Edge, uma versão mais segura e atualizada do Internet Explorer 8, os testes foram realizados porém não foi possível capturar nenhum usuário e senha.

Teste 3 – com Zenmap

O terceiro teste foi realizado a partir dos *softwares* Nmap e Zenmap, com o objetivo de identificar as portas e serviços abertos em dispositivos da rede. Estes softwares têm como objetivo mapear a rede e também é possível gerar a topologia da mesma.

Para este teste foi utilizado o comando “nmap -T5 -A -v” e IP e mascará da rede alvo, onde “-T5” é para acelerar a varredura e também para verificar se existem mecanismos de segurança na rede, já que este teste faz barulho na rede, ou seja, pode ser identificado; “-A” para detectar o sistema operacional e versão dos *hosts*, também para traçar uma rota; “-v” para ativar o modo *verbose* que fornece mais informações sobre os *hosts*, conforme a Figura 40.

Figura 40: Definição de alvos no Zenmap



Fonte: O autor

No ambiente acadêmico foi possível identificar duas portas e serviços abertos, sendo uma no *host* 192.168.100.66 e outra no *host* 192.168.100.206, conforme as Figuras 41 e 42.

Figura 41: Portas e serviços abertos no host 192.168.100.66

```
Nmap scan report for 192.168.100.66
Host is up (0.11s latency).
Not shown: 904 closed ports, 95 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     Dropbear sshd 2013.59 (protocol 2.0)
MAC Address: 04:18:D6:0A:9D:8A (Ubiquiti Networks)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.24 - 2.6.36
```

Fonte: O autor

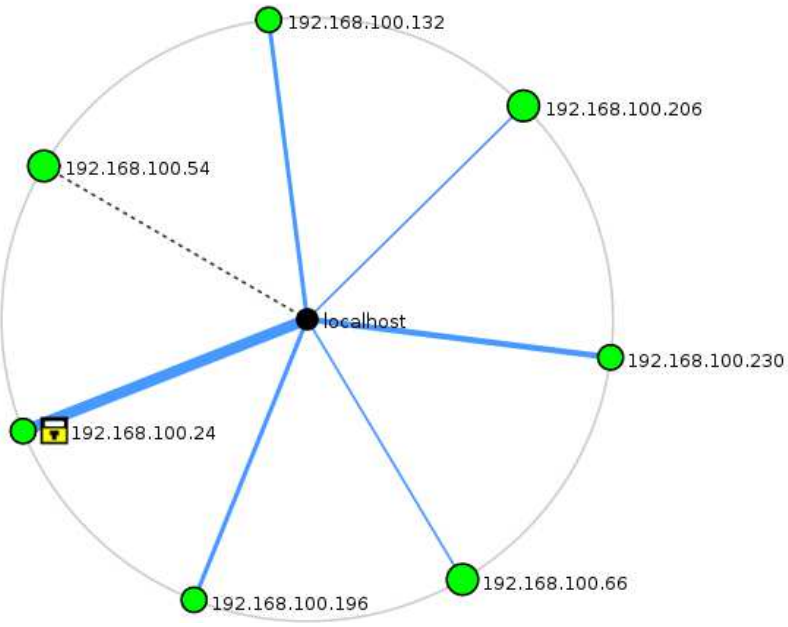
Figura 42: Portas e serviços abertos no host 192.168.100.206

```
Nmap scan report for 192.168.100.206
Host is up (0.11s latency).
Not shown: 909 closed ports, 90 filtered ports
PORT      STATE SERVICE    VERSION
62078/tcp open  tcpwrapped
MAC Address: 28:E1:4C:02:D5:DF (Apple)
OS details: Apple Mac OS X 10.7.0 (Lion) - 10.11 (El Capitan) or iOS 4.1 - 9 (Darwin 10.0.0 - 15.0.0)
Uptime guess: 0.483 days (since Fri Oct 14 08:42:27 2016)
```

Fonte: O autor

Também foi possível realizar a topologia desta rede, conforme a Figura 43.

Figura 43: Topologia do ambiente acadêmico



Fonte: O autor

No ambiente público, com este teste, foi possível apenas identificar as portas e serviços que estavam funcionando no roteador de borda, no AP e no dispositivo por

onde estava sendo realizado o teste, conforme citado na seção 2.3.3, isto ocorre devido a técnica de isolamento AP.

No roteador de borda foi possível identificar as seguintes portas e serviços, conforme a Figura 44.

Figura 44: Portas e serviços abertos no roteador de borda (192.168.12.1)

```
Nmap scan report for 192.168.12.1
Host is up (0.035s latency).
Not shown: 976 closed ports
PORT      STATE    SERVICE         VERSION
22/tcp    open     tcpwrapped
33/tcp    filtered dsp
1032/tcp  filtered iad3
1085/tcp  filtered webobjects
1093/tcp  filtered proofd
1233/tcp  filtered univ-appserver
1352/tcp  filtered lotusnotes
1658/tcp  filtered sixnetudr
2000/tcp  open     bandwidth-test MikroTik bandwidth-test server
2005/tcp  filtered deslogin
3372/tcp  filtered msdtc
3918/tcp  filtered pktcablemmcops
5718/tcp  filtered dpm
5988/tcp  filtered wbem-http
6547/tcp  filtered powerchuteplus
6565/tcp  filtered unknown
8045/tcp  filtered unknown
8291/tcp  open     tcpwrapped
9593/tcp  filtered cba8
10003/tcp filtered documentum_s
10629/tcp filtered unknown
12000/tcp filtered cce4x
35500/tcp filtered unknown
52848/tcp filtered unknown
MAC Address: D4:CA:6D:E8:C4:31 (Routerboard.com)
Device type: general purpose
Running: Linux 2.6.X|3.X
```

Fonte: O autor

No AP foi possível identificar as seguintes portas e serviços, conforme a Figura 45.

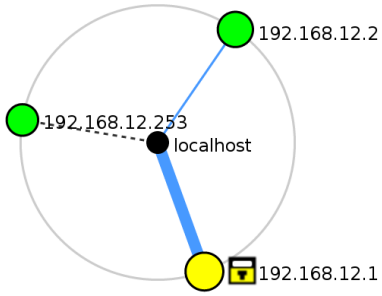
Figura 45: Portas e serviços abertos no AP (192.168.12.2)

```
Nmap scan report for 192.168.12.2
Host is up (0.018s latency).
Not shown: 969 closed ports, 29 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     Dropbear sshd 2014.63 (protocol 2.0)
80/tcp open  http    lighttpd 1.4.35
|_http-favicon: Unknown favicon MD5: 6DCAB71E60F0242907940F0FCDA69EA5
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: lighttpd/1.4.35
| http-title: Error 404 - Page Not Found
|_Requested resource was /nocookies.html
MAC Address: 68:72:51:42:29:7D (Ubiquiti Networks)
Device type: general purpose|WAP
Running: Linux 2.6.X, Ubiquiti AirOS 5.X
```

Fonte: O autor

Também foi possível realizar a topologia desta rede, conforme a Figura 46.

Figura 46: Topologia do ambiente público



Fonte: O autor

No ambiente comercial, foi possível perceber que por meio deste teste, o AP bloqueia as requisições dizendo que o *host* expirou, conforme a Figura 47, sendo apenas possível identificar as portas e serviços apenas do próprio dispositivo de onde está sendo realizado o teste, conforme a Figura 48.

Figura 47: Bloqueio de requisições no ambiente comercial

```
Skipping host 10.90.109.133 due to host timeout
Nmap scan report for 10.90.109.144
Host is up (0.048s latency).
Skipping host 10.90.109.144 due to host timeout
Nmap scan report for 10.90.109.155
Host is up (0.065s latency).
Skipping host 10.90.109.155 due to host timeout
Nmap scan report for 10.90.109.232
Host is up (0.12s latency).
Skipping host 10.90.109.232 due to host timeout
Nmap scan report for 10.90.109.237
Host is up (0.061s latency).
Skipping host 10.90.109.237 due to host timeout
```

Fonte: O autor

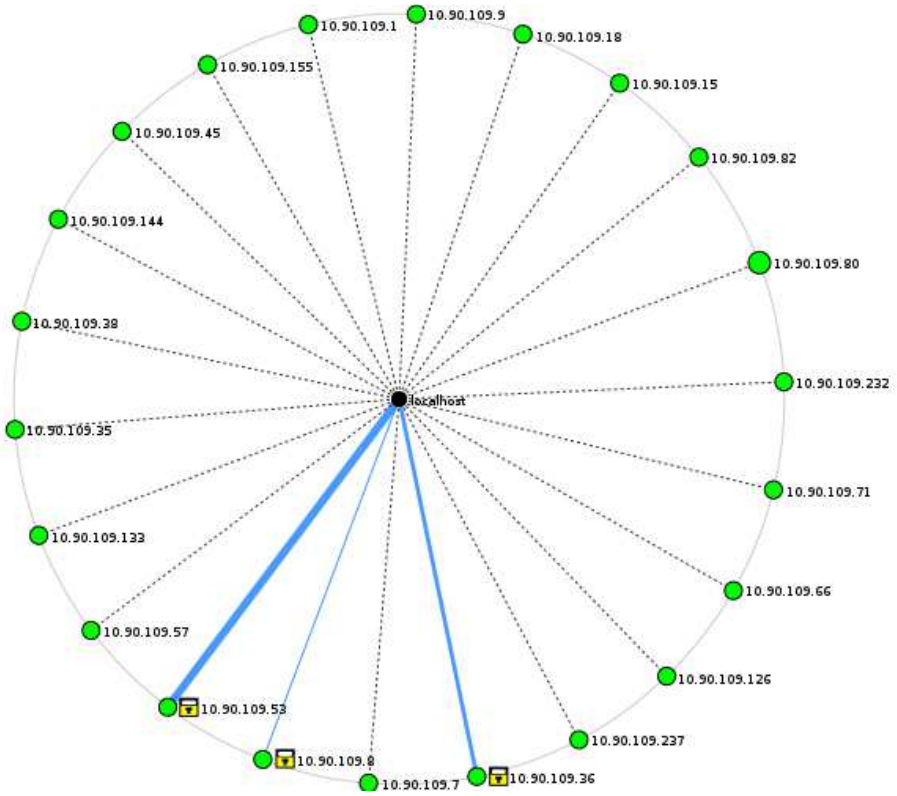
Figura 48: Portas e serviços abertos no dispositivo testador (192.90.109.80)

```
Nmap scan report for 10.90.109.80
Host is up (0.000034s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE VERSION
111/tcp open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4        111/tcp  rpcbind
|   100000  2,3,4        111/udp  rpcbind
|   100024  1          47882/tcp  status
|_  100024  1          51583/udp  status
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.8 - 4.5
```

Fonte: O autor

Porém, ainda foi possível realizar a topologia da rede, conforme a Figura 49.

Figura 49: Topologia do ambiente comercial



Fonte: O autor

No ambiente de saúde foi possível perceber que a rede cabeada é ligada a rede sem fio, devido a quantidade de *hosts* existentes e também as portas que estavam abertas, conforme a Figura 50.

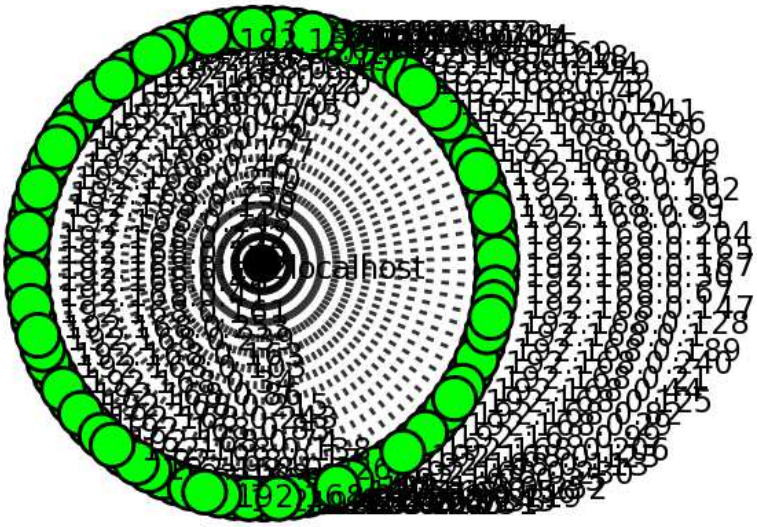
Figura 50: Portas descobertas no ambiente de saúde

```
Discovered open port 25/tcp on 192.168.0.163  Discovered open port 143/tcp on 192.168.0.34  Discovered open port 119/tcp on 192.168.0.142
Discovered open port 587/tcp on 192.168.0.28  Discovered open port 143/tcp on 192.168.0.94  Discovered open port 119/tcp on 192.168.0.59
Discovered open port 993/tcp on 192.168.0.36  Discovered open port 143/tcp on 192.168.0.126 Discovered open port 119/tcp on 192.168.0.101
Discovered open port 587/tcp on 192.168.0.137 Discovered open port 110/tcp on 192.168.0.123 Discovered open port 119/tcp on 192.168.0.117
Discovered open port 587/tcp on 192.168.0.138 Discovered open port 110/tcp on 192.168.0.99  Discovered open port 119/tcp on 192.168.0.128
Discovered open port 25/tcp on 192.168.0.143  Discovered open port 110/tcp on 192.168.0.101 Discovered open port 119/tcp on 192.168.0.124
Discovered open port 587/tcp on 192.168.0.161 Discovered open port 110/tcp on 192.168.0.84  Discovered open port 119/tcp on 192.168.0.123
Discovered open port 587/tcp on 192.168.0.1   Discovered open port 110/tcp on 192.168.0.161 Discovered open port 119/tcp on 192.168.0.109
Discovered open port 993/tcp on 192.168.0.21  Discovered open port 110/tcp on 192.168.0.10  Discovered open port 119/tcp on 192.168.0.82
Discovered open port 993/tcp on 192.168.0.30  Discovered open port 110/tcp on 192.168.0.76  Discovered open port 119/tcp on 192.168.0.105
Discovered open port 993/tcp on 192.168.0.33  Discovered open port 110/tcp on 192.168.0.63  Discovered open port 119/tcp on 192.168.0.1
```

Fonte: O autor

Também foi possível realizar a topologia desta rede, conforme a Figura 51.

Figura 51: Topologia no ambiente de saúde



Fonte: O autor

4 DISCUSSÃO DOS RESULTADOS

Referente ao primeiro teste, realizado com o Fing, foi possível perceber que no ambiente acadêmico é permitido realizar a varredura na rede com o objetivo de identificar os nós participantes da rede. É possível identificar os mesmos através de seu endereço IP, endereço MAC e marca. Também foi possível identificar os serviços que estavam em funcionamento no *switch* principal e redundante, sendo eles o serviço de HTTP na porta 80 que é o serviço de configuração do switch via navegador, o serviço de SSH na porta 22, para acesso remoto e também o serviço de Telnet na porta 23, também para acesso remoto. Neste último serviço existe uma vulnerabilidade onde é possível capturar o pacote na rede contendo o usuário e senha em texto puro e a principal recomendação para mitigação desta vulnerabilidade é de não utilizar este serviço.

No ambiente público também foi possível realizar a varredura na rede, porém somente foi possível encontrar três dispositivos, sendo o roteador de borda, o AP e o próprio *smartphone* de onde foi realizado o teste. Isso ocorre devido a técnica de isolamento AP, que conforme citado na seção 2.3.3, cria uma rede virtual para cada dispositivo conectado à rede. Também foi possível encontrar os serviços que estavam em funcionamento no roteador de borda (192.168.12.1), sendo eles o serviço de SSH na porta 22 e o de callbook na porta 2000, que é um servidor de teste para largura de banda e no AP (192.168.12.2), sendo eles os serviços de HTTP na porta 80 e de SSH na porta 22.

No ambiente comercial, assim como no ambiente acadêmico, foi possível localizar todos os dispositivos na rede e também os serviços que estavam em funcionamento no AP, sendo estes serviços o de HTTP na porta 80 e o de HTTPS na porta 443, que é utilizado para conexão segura a página de configuração.

No ambiente de saúde também foi possível localizar todos hosts, porém não foi possível identificar os serviços que estavam em funcionamento no AP.

Este teste, para os usuários, mostra a importância de se ter um *firewall* pessoal para que portas e serviços abertos não sejam explorados por pessoas mal-intencionadas. Para os administradores de rede, mostra a importância de realizar a configuração correta do AP deixando apenas os serviços necessários em funcionamento.

Referente ao segundo teste, realizado com o Wireshark, nos ambientes acadêmico, comercial e de saúde, foram possíveis capturar os pacotes de todos dispositivos que estavam realizando algo na rede. Porém no ambiente público, somente foi possível capturar pacotes do próprio dispositivo testador.

Também foi possível perceber a importância de utilizar navegadores seguros e atualizados com *patchs* de segurança, pois como demonstrado no teste com o SSLSTRIP, é possível capturar contas e senhas de usuários que utilizam navegadores desatualizados que ainda usam apenas do protocolo de segurança SSL no protocolo HTTPS para realizar a autenticação e manter a confidencialidade e integridade dos dados, por exemplo o Internet Explorer 8 que após ter sido atualizado para uma versão mais segura, no caso o Edge, este tipo de vulnerabilidade foi evitada.

Referente ao terceiro teste, realizado com o Zenmap, foi possível identificar as portas e serviços abertos nos dispositivos que estavam conectados na rede naquele momento. No ambiente acadêmico, foi possível identificar serviços e portas abertas em dois dispositivos, sendo o serviço de SSH na porta 22 no *host* 192.168.100.66 que utiliza Linux como sistema operacional e a porta 62078 no *host* 192.168.100.206 que utiliza iOS como sistema operacional, o serviço desta porta consta como *tcpwrapped*, pois existe alguma proteção para que este não seja descoberto por varreduras.

No ambiente público, foi possível identificar as portas e serviços abertos que estavam no roteador de borda e AP, no primeiro os serviços que estavam abertos eram o de SSH na porta 22, o de *callbook* na porta 2000 e o *tcpwrapped* na porta 8291, o restante das portas aparecem como filtradas devido ao fato de que o Nmap não consegue determinar se a porta está aberta ou fechada, porém é possível perceber os serviços que estão em funcionamento nestas portas.

No ambiente comercial, por existir um mecanismo de segurança ou regras no *firewall* que impedem essa varredura, foi apenas possível identificar os serviços e portas abertas apenas do dispositivo testador, sendo o serviço de rpcbind na porta 111, este é utilizado para realizar a varredura na rede. Além de realizar o mapeamento da rede.

No ambiente de saúde, foi possível identificar na maioria dos *hosts* as portas 25 e 587, sendo estas do serviço SMTP utilizado como serviço padrão para envio de e-mails pela Internet, 143 e 993, sendo estas do serviço IMAP que é utilizado para gerenciamento de e-mails, 110, sendo esta do serviço POP3 que é utilizado para

acesso aos e-mails e 119, sendo esta do serviço NNTP que é utilizado para transferência de informações.

Com a grande quantidade de *hosts* no ambiente de saúde, foi possível notar que a rede sem fio é ligada a rede cabeada, conforme citado na seção 2.3.1., isto pode ser explorado por uma pessoa mal-intencionada.

Através deste teste, é possível perceber a importância de se ter mecanismos de segurança que impedem essa varredura e assim como o primeiro teste, para os usuários, a importância de um *firewall* pessoal.

Para melhorar a segurança de redes sem fio públicas e mitigar ameaças, vulnerabilidades e ataques, uma das configurações mais recomendadas são: separar a rede sem fio da rede cabeada, seja ela por utilização de redes virtuais ou um *link* de Internet separado.

Outra recomendação é, dedicar esta rede totalmente para acesso à Internet, sem a necessidade de compartilhamento de recursos. Para isso, deve-se utilizar a técnica de isolamento AP, que além desta função, também impede outras vulnerabilidades como a varredura na rede ou captura de pacotes, impossibilitando que os dados dos usuários fiquem expostos para pessoas mal-intencionadas.

Também é necessário desabilitar o acesso para as configurações do AP via rede sem fio, tornando necessário se conectar ao mesmo via SSH ou via cabo.

5 CONSIDERAÇÕES FINAIS

Com a simplicidade de implantação de redes sem fio e à necessidade de uso de Internet por parte das pessoas, o número de redes sem fio públicas vem crescendo ao longo dos anos. Com isso, aumenta o número de vulnerabilidades e também o número de pessoas mal-intencionadas que querem explorá-las a fim de conseguirem dados sigilosos das pessoas que utilizam estas redes, devido a facilidade de encontrarem *softwares* que tem este objetivo.

Neste trabalho foi apresentado a segurança da informação, envolvendo seus três princípios base, sendo eles a confidencialidade, a integridade e a disponibilidade. Em relação às redes sem fio, de uma maneira mais ampla, foram levados em consideração aspectos como definição, classificação e seus padrões. Com base na segurança da informação, foi apresentado a segurança utilizada em redes sem fio, considerando antes as ameaças, vulnerabilidades e ataques associados a redes sem fio para depois apresentar as técnicas seguras utilizadas para prevenção dos mesmos, sendo a técnica de isolamento AP a mais importante para o desenvolvimento do trabalho, e também uma técnica voltada para os usuários utilizarem, o *firewall* pessoal.

Através da pesquisa de campo e testes realizados nas redes sem fio dos ambientes acadêmico, público, comercial e de saúde que foi focado no padrão de rede sem fio 802.11 (Wi-Fi), foi possível analisar os métodos de segurança utilizados nos mesmos e também demonstrar possíveis riscos que os usuários podem sofrer estando conectados à estas redes, como a vulnerabilidade no protocolo SSL, que é possível capturar a conta e senha dos usuários em texto puro. Também foi ressaltado à importância de se utilizar um *firewall* pessoal para prevenção de varreduras no seu dispositivo e também atualizá-lo com *patchs* de segurança fornecidas pelos próprios desenvolvedores ou terceiros a fim de extinguir qualquer vulnerabilidade que existe no mesmo.

Viu-se ainda que durante a discussão dos resultados, o ambiente mais seguro dos quatros apresentados, foi o ambiente público que utiliza de uma rede totalmente dedicada à o uso da Internet para seus usuários, utilizando da técnica de isolamento AP que mitiga a maioria das ameaças, vulnerabilidades e ataques citados. E o ambiente menos seguro, foi o ambiente de saúde que utiliza da rede sem fio ligada a rede cabeada sem uma separação, sendo possível identificar todos os *hosts* daquela

faixa tanto da rede sem fio quanto da rede cabeada, tornando os dados do local inseguros.

Na mesma seção, também foi exposto uma configuração para as redes sem fio públicas que procura mitigar todos os tipos ameaças, vulnerabilidades e ataques.

Então, conclui-se que o objetivo proposto foi alçando mostrando a importância de ser atenção a quais redes uma pessoa pode se conectar e também que se uma rede pública for configurada de maneira correta, como a rede sem fio do ambiente público, é seguro usá-la.

Durante a elaboração deste trabalho, foi visto que existem outras possibilidades de pesquisa que podem agregar valor ao mesmo, sendo elas:

- Desenvolvimento de uma política de segurança para rede sem fio com foco em redes sem fio públicas;
- Análise de segurança no padrão 802.11 (Bluetooth);
- Análise de segurança no padrão 802.16 (WiMax) e também nas tecnologias similares como o Projeto Loon e Internet.org;
- Implantação de um sistema de rede sem fio pública utilizando a tecnologia OpenWrt e sistema de Vouncher.

Assim, estes itens citados podem ser abordados em trabalhos futuros.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Presidência da República. *In.:* **Planalto.gov.br.** Brasília/DF, 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm>. Acessado em: 20 out. 2016.

CERT. **Cartilha de segurança para Internet.** 2012. Disponível em: <http://cartilha.cert.br/>. Acessado em: 11 set. 2016.

CISCO. **Exemplo de configuração do acesso protegido por wi-fi 2 (wpa2).** 2016. Disponível em: <https://www.cisco.com/cisco/web/support/BR/104/1043/1043935_wpa2_config.pdf>. Acessado em: 25 set. 2016.

CUTRIM, Carlos M. O. **Segurança em redes:** segurança em redes sem fio**.** 2013. Monografia (Especialização em Segurança da Informação), SENAC do Distrito Federal – FACSENAC/DF. Disponível em: <http://www.edilms.eti.br/uploads/file/orientacoes/seg02%20Carlos%20Magno%20de%20Oliveira%20Cutrim-TCC-final.pdf>. Acessado em: 25 set. 2016.

DSIC. Departamento de Segurança da Informação e Comunicações. **Segurança da informação.** 2009. Disponível em: <http://dsic.planalto.gov.br/seguranca-da-informacao>. Acessado em: 23 mai. 2016.

ETTERCAP**.** Disponível em: <https://ettercap.github.io/ettercap>. Acessado em: 20 out. 2016.

FING**.** Disponível em: <https://www.fing.io>. Acessado em: 10 out. 2016

FUROUZAN, Behrouz A. **Comunicação de dados e redes de computadores.** 4 ed. São Paulo: AMGH Editora Ltda, 2008.

IEEE. **Standards ieee 802.11**. 2012. Disponível em: <http://standards.ieee.org/about/get/802/802.11.html>. Acessado em: 14 jun. 2016.

IEEE. **Standards ieee 802.15**. 2005. Disponível em: <http://standards.ieee.org/about/get/802/802.15.html>. Acessado em: 27 ago. 2016.

IEEE. **Standards ieee 802.16**. 2012. Disponível em: <http://standards.ieee.org/about/get/802/802.16.html>. Acessado em: 27 ago. 2016.

INTERNET.ORG**.** 2013. Disponível em: <https://info.internet.org/pt/>. Acesso em: 24 set. 2016

KUROSE, Jim F; ROSS, Keith W. **Rede de computadores e a internet:** uma abordagem top-down. 5 ed. São Paulo: Pearson Education, 2010.

LYNKSIS. **Isolamento de ap e como habilitar/desabilitar o isolamento de ap. (**[s.d]). Disponível em: <http://www.linksys.com/br/support-article?articleNum=135098>. Acessado em: 25 set. 2016.

NMAP**.** Disponível em: <https://nmap.org/>. Acessado em: 10 out. 2016.

PROJETO LOON. 2013. Disponível em: <https://www.google.com/intl/pt-BR/loon/>. Acessado em: 24 set. 2016.

RAMALHO, Vitor Gomes. **Uma comparação entre os protocolos de roteamentos mr-lqsr e aodv.** 2014. Dissertação (Mestrado em Ciência da Computação). Universidade Federal de Viçosa. Disponível em: <http://www.locus.ufv.br/handle/123456789/2674>. Acessado em: 28 ago. 2016.

SHIREY, R. **RFC 2828:** internet security glossary. 2000. Disponível em: <https://www.ietf.org/rfc/rfc2828.txt>. Acessado em: 08 mai. 2016.

RUFINO, Nelson Murilo de Oliveira. **Segurança em redes sem fio.** 4. ed. São Paulo: Novatec, 2014.

SÊMOLA, Marcos. **Gestão da segurança da informação:** uma visão executiva. 2. ed. Rio de Janeiro: Elsevier, 2014.

SOUZA, Fabrício R. A.; SILVA, Cristiano M. da; GUIMARÃES, Cayley. **Segurança em redes wireless**. 2009. Artigo Científico. Centro Universitário de Belo Horizonte - UniBH. Disponível em: <http://revistas.unibh.br/index.php/dcet/article/viewFile/236/128>. Acessado em: 10 mai. 2016.

STALLINGS, William. **Criptografia e segurança de redes:** princípios e práticas. 6 ed. São Paulo: Person Education, 2014.

STEINHAUSER, Paulo L. **Ziglar - utilização de redes sem fio zigbee para acessibilidade aos portadores de deficiência física.** 2013. Artigo Científico. Universidade do Alto Vale do Itajaí. Disponível em: <http://www.uniedu.sed.sc.gov.br/wp-content/uploads/2013/10/Paulo-Luis-Steinhauser.pdf>. Acessado em: 10 set. 2016.

SSLSTRIP**.** Disponível em: <https://moxie.org/software/sslstrip/>. Acesso em 20 out. 2016.

TANENBAUM, Andrew S. **Rede de computadores.** 5 ed. São Paulo: Pearson Education, 2011.

TANENBAUM, Andrew S. **Sistemas operacionais modernos.** 3 ed. São Paulo: Pearson Education, 2010.

VILELA, Douglas W. F. L. **Segurança em redes sem fio: estudo sobre desenvolvimento de conjunto de dados para comparação de ids.** 2014. Dissertação (Mestrado em Engenharia Elétrica). Faculdade de Engenharia – UNESP – Campus de Ilha Solteira. Disponível em: <http://repositorio.unesp.br/handle/11449/124423>. Acessado em: 04 set. 2016.

WI-FI ALLIANCE. Disponível em: <https://www.wi-fi.org>. Acessado em: 13 set. 2016.

WIRESHARK. Disponível em: <https://www.wireshark.org>. Acessado em: 10 out. 2016.

ZENMAP. Disponível em: <https://nmap.org/zenmap>. Acessado em: 10 out. 2016.