A UTILIZAÇÃO DE SOFTWARE LIVRE PARA ANÁLISE DE VULNERABILIDADES EM REDES WIRELESS EM SHOPPINGS CENTERS DE SÃO LUÍS - MA UTILIZANDO A TÉCNICA DO WARDRIVING.

Bruno Emanuel Setúbal Learte, contato@brunosi.com.br
Will Ribamar Mendes Almeida, will75@gmail.com

[1] Universidade CEUMA, Rua Josué Montello, nº 1, Renascença II - São Luís – MA.
[2] Faculdade Laboro São Luís-MA, Av. Castelo Branco, São Francisco - São Luís MA.

Resumo. Avanços tecnológicos nas redes sem fio ao longo do tempo permitiram o rápido compartilhamento de informações em qualquer lugar e horário. A facilidade na captação dos sinais através da utilização da técnica wardriving e domínio de ferramentas de invasões facilitam o processo de roubo de informações. Sendo assim, este artigo tem por objetivo realizar testes de invasões em redes sem fio que utilizam protocolos de criptografia (WEP, WPA e WPA2) e mapear o quantitativo de redes que utilizam deste tipo de mecanismo de segurança nos cinco grandes shoppings de São Luís - MA. A partir da consolidação dos dados, apresentam-se à sociedade os resultados obtidos com o intuito de relatar a situação atual em relação à segurança da informação nestes locais.

Palavras-chave: Wardriving; redes sem fio; segurança da informação.

OUTROS TRABALHOS EM:
www.projetoderedes.com.br

1. INTRODUÇÃO

A Sociedade da Informação teve a sua evolução no berço da Segunda Guerra Mundial e seu apogeu durante a Guerra Fria, com as revoluções técnicas e cientificas que ocorreram durante o período entre 1939 e 1960, houve o advento de novas tecnologias tais como: novos sistemas de comunicação, criação de processadores analógicos de dados (computadores primitivos) e inovação a partir do projeto ARPANET (projeto piloto da internet) (SARACEVIC, 1966, p.56).

Com o constante avanço das tecnologias de compartilhamento das informações, houve a necessidade de conectividade para acesso aos dados em tempo real, com maior mobilidade, flexibilidade e disponibilidade que levaram ao avanço das tecnologias de comunicação sem fio. Tais revoluções trazem consigo a constante necessidade da segurança em redes. Importância esta que surge pelo fato de informações valiosas estarem trafegando sem qualquer tipo de gestão ativa, ficando estes sujeitos a ataques.

Embora os avanços nas últimas décadas na área da segurança da informação em redes sejam expressivos, uma rede sem fio (*wireless*) não é completamente segura. Em um universo globalizado e competitivo, as informações são os ativos mais importantes de qualquer setor. Falhas de configurações, posicionamento inadequado do ponto de acesso à rede sem fio ou falta de conhecimento das ameaças são fatores agravantes para o aumento do risco de invasões e que podem gerar prejuízos irrecuperáveis. Ademais, com a facilidade de captação do sinal de redes sem fio, aliado à necessidade de proteção dos dados nelas trafegados, questiona-se o real nível de proteção destas e quais as melhores práticas para o fortalecimento da segurança da informação em redes. Levando em consideração as ideias anteriores, este trabalho tem como objetivo analisar o nível vulnerabilidades das redes sem fio nos principais shoppings centers em São Luís no Estado do Maranhão e, a partir desses resultados, apresentar a sociedade os riscos envolvidos na utilização deste tipo de comunicação.

Neste trabalho é realizado é o processo de levantamento de informações das redes sem fio utilizando a técnica wardriving. Esta técnica normalmente utiliza um carro, um amplificador de sinais, um notebook e softwares como ferramenta para identificação, análise e teste de invasão nos protocolos de criptografia redes investigadas. Para tal, é levada em consideração a necessidade dos estudos relacionados às tecnologias das redes sem fio, o processo de transmissão de dados entre equipamentos, os modos de operações, os padrões utilizados e os métodos de invasões em redes wireless “protegidas”, para, assim, obter resultados que possibilitem mapear a quantidade de pontos de acesso encontrados nestes locais e o nível de proteção dos mesmos.

2. DEFINIÇÕES PRELIMINARES

2.1. Segurança da Informação.

De acordo com Peixoto (2006, p. 37):

> O termo segurança da informação pode ser designado como uma área do conhecimento, informático ou não, que salvaguarda os chamados ativos de informação, contra acessos indevidos, modificações, não autorizadas ou até mesmo sua não disponibilidade.

A Segurança da Informação está relacionada com a proteção existente ou necessária sobre dados que possuem valor para alguém ou para uma organização. Na Figura 1 são demonstrados os pilares da Segurança da Informação.

Figura 1 – Os pilares da Segurança da Informação
FONTE: ALVES, 2006, p. 29.

A confidencialidade, a integridade, a disponibilidade e seus complementares, autenticidade e o não repúdio. São os conceitos básicos considerados como pilares da segurança da informação. As suas características são abordadas a seguir:

a) Confidencialidade: É a característica referente à garantia de que as informações alcançaram o seu destino final, sem que dissipem para outro lugar onde não deveria passar.
b) Integridade: É a propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação original.
c) Disponibilidade: É característica que corresponde à garantia que a informação esteja sempre disponível para uso legitimo, ou seja, informações ou sistemas informáticos resistentes a falhas.
d) Não Repúdio e Autenticidade: Também conhecido como responsabilidade final, e tem como objetivo verificar a identidade e autenticidade de alguém ou até mesmo de um agente exterior a fim de garantir a integridade de origem.

O vazamento de informações pessoais e corporativas é uma crescente que causa prejuízos imensuráveis, por exemplo, um simples clicar pode abrir portas para um mundo de exploração de malfeitores. O momento é bastante preocupante: ataques e roubos de informações a órgãos públicos e privados são a moda da época, além da onda de *hacketivismo* proposto por um grupo principal, denominado *anonymous*. A mídia vem tentando alertar a sociedade, aprofundando-se cada vez mais no assunto a fim de criar um conhecimento mais consolidado, entretanto, pouco tem sido feito a sociedade para proteger a sociedade e as suas informações.

Recentes revelações sobre a espionagem cibernética entre nações demonstra que a fronteira entre ataque e defesa pode ser tênue. Segundo entrevista realizada com especialistas de segurança pela BBC Brasil (14 de outubro, 2013), “nenhum país ou pessoa está 100% protegido da ação de *hackers*, sejam eles ativistas, integrantes de grupos criminosos ou funcionários de inteligência de outras organizações/países”. Assim, verifica-se que a informação é um ativo que precisa ser protegido, e é essencial para as pessoas ou negócios de uma organização. Desenhar, alcançar, manter e melhorar a segurança das informações é atividades essenciais para assegurar a proteção dos dados.

2.2. A tecnologia das redes sem fio.

Segundo Lucchese (2007, p.23):

> Redes *Wireless* (sem fio), em particular as redes *Wi-fi (Wireless Fidelity)* tornam-se, sem dúvida, cada dia mais populares e imprescindíveis, sendo inegável a necessidade da sua utilização em lugares como aeroportos, hotéis, cafés, etc. As redes *wireless* propiciam uma considerável praticidade e mobilidade em ambientes corporativos e/ou domésticos são capazes de mudar a maneira como as pessoas trabalham e permanecem distantes de sua base habitual.

O termo *wireless* é caracterizado pela sem utilização de cabos, ou seja, pela transmissão de informação através do ar. Neste modelo de comunicação, podem-se citar várias tecnologias como: *Bluetooth*, *Wi-fi* e infravermelho. Para que o processo de transporte de dados ocorra por meio de uma rede *wireless*, é necessário o envolvimento de quatro elementos: o meio físico de transmissão, a estrutura da rede, o modo de operação e o padrão a ser utilizado. Estes serão resumidamente abordados a seguir:

a) Meios de Transmissão: A transmissão em rede sem fio pode ser dividido em quatro grandes grupos: *laser*, radiofrequência, micro-ondas e infravermelho. Cada um destes meios de transmissões possui um conjunto de limitações funcionais que são levadas em consideração durante o projeto e a montagem de uma rede.
b) Estrutura da Rede: Uma rede sem fio é um sistema que interliga vários equipamentos fixos ou móveis, visando organizar e facilitar o controle destes durante sua utilização e seu o crescimento. Algumas estruturas foram classificadas quanto ao seu dimensionamento. A WLAN (*Wireless Local Área Network*) é uma rede sem fio de computadores local, segmentada ou não a uma rede LAN cabeada. A estrutura de rede WPAN (*Wireless Personal Área Network*) possui vários tipos de dispositivos móveis conectados a um ponto de acesso de pequeno alcance. Já a WMAN *(Wireless Metropolian Area Network)* também é conhecida por utilizar banda larga, com a utilização de estruturas como torres e satélites.
c) Modo de Operação: Em termos organizacionais, existem dois modos de operação: *Ad-Hoc* e infraestrutura. No caso das redes sem fio que operam em modo *Ad-Hoc* são redes de computadores em que os equipamentos conectam-se diretamente uns aos outros ou com propósitos específicos. As redes sem fio que trabalham com a operação em infraestrutura tem basicamente o ponto de acesso como equipamento central de uma rede, onde o mesmo desempenha a função de *bridge* (ponte) para facilitar a interligação com a rede cabeada.
d) Padrões: As redes sem fio utilizam de padrões técnicos aprovados pelo IEEE (*Institute of Electrical and Electronic Engineers*), o IEEE é uma associação profissional técnica com o objetivo de desenvolver padrões para as áreas de engenharias eletrônicas e computação. Uma das suas principais frentes de trabalho é o padrão denominado 802.11, que segundo Rufino (2005, p. 30), "reúne uma série de especificações que basicamente definem como é feita a comunicação entre um dispositivo cliente e um concentrador ou a comunicação entre dois dispositivos".

2.3. Mecanismos de Segurança.

O conhecimento aprofundado de mecanismos de segurança em rede sem fio são fatores que contribuem para obtenção de um nível mais elevado de segurança. Para o desenvolvimento deste trabalho se faz necessário o entendimento mais aprofundado das tecnologias de segurança em redes. O desenvolvimento da criptografia foi acompanhado pelo desenvolvimento das técnicas de comunicação, onde diversos padrões e políticas de criptografia surgiram e evoluíram principalmente nos meios computacionais. Os três tipos de criptografias que atualmente estão sendo utilizada, são: WEP (*Wired Equivalent Privacy),* WPA (*Wi-fi Protected Access) e* WPA2 (*IEEE 802.11i*). Estas são abordadas de forma sucinta:

a) WEP: Introduzido no padrão IEEE 802.11 em 1999, esta tipo de criptografia provê dois métodos de autenticação de dispositivos. No primeiro utiliza o algoritmo de criptografia RC4 (*Ron's Code #4)* para prevenir a leitura de dados dos usuários e no segundo utiliza o CRC-32 (*Cyclilc Redundancy Cheks*) para verificação da integridade dos dados;
b) WPA: O WPA surgiu com o objetivo principal de corrigir o grande número de vulnerabilidades apresentadas pelo protocolo WEP. As principais características da criptografia do tipo WPA são: o não suporte a operações *Ad-Hoc,* trabalha em modos distintos de autenticidade para redes pessoais e coorporativas, utiliza uma mensagem para verificação de integridade chamada de MIC (*Message Integrity Check)* e trabalha com o conceito de chaves temporais (*Pairwise Master Key, PMK)* derivadas outras chaves de integridade e criptografia de dados;
c) WPA2: O WPA2 herdou o dispositivo de autenticação do WPA, tendo apenas como avanço no processo de autenticação o desenvolvimento do *roaming.* Segundo Linhas e Gonçalves (2008) apud Rockenbach (2008), "a confidencialidade e a integridade do protocolo WPA2 são garantidas pelo protocolo CCMP (*Counter-Mode/Cipher Block Chaining Message Authentication Code Protocol*)";

Segundo Rockenbach (2008), "o protocolo CCMP utiliza o padrão de criptografia simétrico AES (*Advanced Encryption Standard)* para fornecer uma criptografia mais segura". De acordo com Rocha (2006: 34), "o AES permite a utilização das chaves de 128, 192 ou 256 bits e trabalha como diferentes modos de operação, que alteram a forma como o processo de criptografia é realizado".

2.4. A técnica do *Wardriving*.

> *Wardriving* é o ato de mover-se ao redor de uma área especifica e mapear a população de pontos de acesso *wireless* para um propósito estatístico. Estas estatísticas são então utilizadas para elevar a atenção sobre problemas de segurança associados a estes tipos de rede (tipicamente *wireless*). (HURLEY ET AL, 2004, p.12).

Esta técnica foi desenvolvida em abril de 2001 por Peter Shipley. Diferentemente de outros que precisavam correr com *laptops*, lendo e tomando notas sobre os pontos de acessos encontrados, Peter automatizou o processo com software dedicado com integração de dos dados de localização GPS com bancos de dados dos pontos de acessos detectados. Com base nessa necessidade algum tempo depois Marius Milner NetStumbler desenvolveu uma ferramenta popular para a prática do *wardriving*, o *NetStumbler*.

O termo “*war”* de *wardriving* não tem nada haver com guerra. O termo é descendência do *wardialing*, que era a prática de discar números de telefone aleatórios por meio do computador com o intuito de identificar modens disponíveis para acesso a Internet. O *wardriving* proporciona uma oportunidade para avaliar o crescimento de um segmento de mercado de tecnologia ou para efetuar avaliações de segurança de redes. Este poderá ser considerado como um conjunto de métodos que auxiliam na identificação das redes sem fio, capturam os pacotes e analisam informações que possibilitem o acesso as redes.

Do ponto de vista histórico a técnica é um tanto quanto antiga; entretanto, as redes sem fio em locais públicos só passaram a ganhar grandes proporções a partir do barateamento dos pontos de acesso, ou seja, a partir de 2009. Tal acontecimento gerou interesse de *cyber* criminosos, causando uma maior procura por técnicas como o *wardriving* e ferramentas específicas.

3. ESTUDO DE CASO

3.1. Materiais e Métodos

O principal objetivo deste trabalho é avaliar e analisar o grau de vulnerabilidades das redes sem fio em 5 (cinco) grandes *shoppings* da cidade de São Luís do Estado do Maranhão. Por questões éticas os nomes dos *shoppings* não serão referenciados ao longo desta pesquisa.

A metodologia adotada foi o levantamento bibliográfico, pois, segundo Martins (2007, p.35), “se vale de estudo para conhecer as contribuições cientificas sobre determinado assunto”. Esta se caracteriza como exploratória porque, na concepção de Gil (2008, p.27), “busca proporcionar visão geral, de tipo aproximativo, acerca de determinado fato”, já que ao longo do estudo o tema será explorado e aplicado de forma a proporcionar um rico conhecimento.

Para o desenvolvimento da proposta inicialmente efetuou-se testes de invasão em redes sem fio que utilizam as criptografias: WEP, WPA e WPA2. A partir dos resultados obtidos, verificaram-se quais tipos de criptografias foram as mais seguras. O segundo passo foi utilizar a técnica do *wardriving* para chegar ao quantitativo de redes sem fio de cada um dos 5 (cinco) *shoppings centers* analisados, apresentando as características de cada um dos pontos de acessos identificados.

De dentro de um veiculo automotor foi efetuada a movimentação ao redor e nas proximidades da área física dos *shoppings analisados.* Também foram necessários pontos internos fixos para aquisição de informações que não foram detectadas externamente. Sendo assim possível determinar a quantidade total de pontos de acessos às redes sem fio nestes locais. Após a identificação dos pontos de acessos, foram utilizados alguns *softwares* para consolidar os resultados das varreduras. A partir deste levantamento foi realizado o cruzamento da quantidade de redes sem fio identificadas com os seus respectivos tipos de tecnologia de criptografia.

3.1.2. Equipamentos utilizados.

Para a realização dos testes nos ambientes de redes sem fio, foi utilizado além do automóvel, um *notebook DELL INSPIRION*. Na Tabela 1 são apresentas as especificações do equipamento utilizado:

Tabela 1. Especificações do equipamento utilizado.

Sistema Operacional	*KALI LINUX 2.0 2016.2*
Memória	8 Gb
Adaptador de rede *Wireless*	Atheros Communications Inc. AR9285 *Wireless* Network Adapter (PCI-Express)
Processador	Intel@ Core i7 4500U CPU @ 1.8GHz x4

3.1.3. Ferramentas utilizadas.

As ferramentas utilizadas para identificação e mapeamento das redes locais, são as seguintes:

a) KALI LINUX 2.0 2016.2: O Kali Linuz é um sistema operacional *Linux* baseado no Debian, com mais de 300 ferramentas para estudos e análise, focados em testes de invasões e auditoria de segurança da informação;

b) Gerenciador *inSSIDer:* É um gerenciador de conexões utilizado durante a prática do *wardriving.* Com ele é possível efetuar uma varredura de busca das redes sem fio ao alcance da antena da máquina hospedeira, captando a força do sinal em intervalos de tempo definidos e ainda determina durante a varredura todas as especificações lógicas da rede, inclusive o tipo de criptografia utilizada;

c) Kismet: É uma ferramenta para identificar e analisar a segurança de redes *wireless.* É capaz de encontrar redes que estão ocultas (ESSID não divulgado);

d) *Aircrack:* É uma *suíte* de aplicações poderosa, capaz de efetuar uma análise de tráfego para auditoria em redes sem fio. Através dos pacotes coletados é possível efetuar a quebra da criptografia das redes sem fio (WEP, WPA e "WPA2");

e) *Reaver:* Uma ferramenta capaz de comprometer a segurança de redes com criptografia WPA/WPA2, considerada a mais forte atualmente. A quebra de segurança acontece em cima da tecnologia WPS (*Wi-fi Protected Setup*) utilizada em equipamentos SOHO (*Small Office – Home Office*)

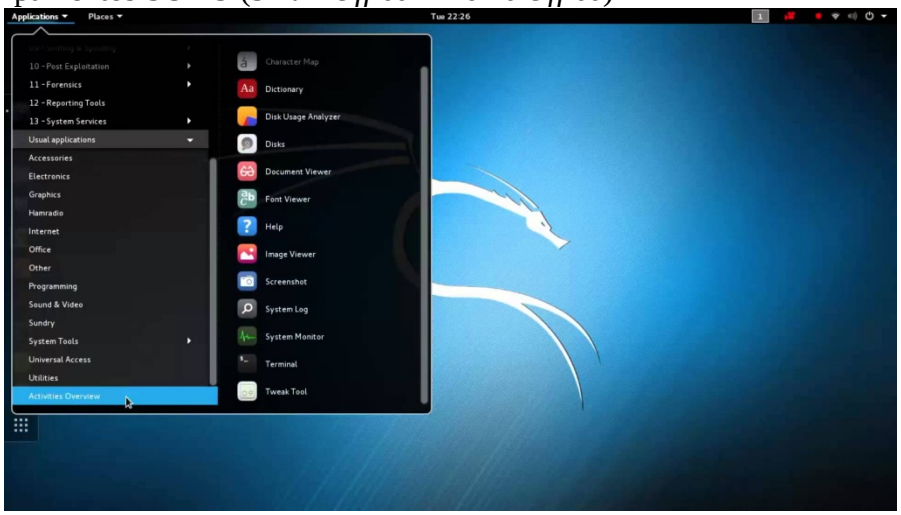

Figura 1. Tela inicial do Kali Linux 2.0

3.2. Resultados

3.2.1. Resultados – Vulnerabilidades nos protocolos de criptografia

Nesta etapa foram realizados testes de invasão em algumas das redes sem fio dos *shoppings,* tendo por objetivo obter uma amostragem dos protocolos de criptografia e evidenciar as suas vulnerabilidades. As redes sem fio analisadas como experimento foram: uma rede sem fio com criptografia WEP encontrada no *shopping Center* A, outra WPA escolhida no *shopping* B e uma terceira com criptografia WPA2 escolhida no *shopping Center* C.

a) Tentativa de quebra da chave WEP no *shopping Center* A.

Muitos pontos de acesso, principalmente os antigos, utilizam versões do WEP, que são as mais fáceis de quebrar. Nesta etapa, é demonstrado o processo de quebra de criptografia WEP.

O primeiro passo é executar o *Kismet* para obter informações da rede sem fio como: SSID e BSSID (nome da rede sem fio de serviço), endereço MAC (endereço físico Da.(Interface de comunicação) de alguns clientes do ponto de acesso selecionado, o canal do ponto de acesso e o tipo de encriptação da rede, no caso, o WEP.

O próximo passo é necessário abrir outro terminal. O objetivo agora é falsear o endereço MAC de sua placa de rede com a do ponto de acesso à rede intencionada.

3º – Abrir o terminal do *KALI LINUX 2.0* e executar o seguinte comando:

 # ifconfig wlan0 down

// ”derrubar” a placa *wireless* para poder trocar o endereço MAC da placa de rede.

4º – O comando a seguir vai permitir falsear o endereço MAC:

 # macchanger -m 00:23:e5:1b:df:0d wlan0

5º – Se o *Kismet* não estiver executando automaticamente a placa de rede em modo de monitoramento (também conhecido como promíscuo), torna-se necessário executar o comando para coloca-la em modo monitor:

 # airmon-ng start wlan0

// caso o comando anterior não seja executado, é porque o *Kismet* já está executando a placa em modo de monitoramento.

6º – Nesta etapa foi executado o comando *aireplay* somente para gerar uma quantidade suficiente de tráfego na rede, tal comando servirá para gerar pacotes mais rapidamente, diminuindo o tempo para quebra da criptografia:

 # aireplay-ng -2 -p 512 -c ff:ff:ff:ff:ff:ff -b <BSSID> -h <MAC falseado> wlan0

// as partes em destaque devem ser substituídas pelas informações obtidas pelo *Kismet.* Ficando assim:

 # aireplay-ng -2 -p 512 -c ff:ff:ff:ff:ff:ff -b 00:23:69:fa:9e:d1
-h 00:23:e5:1b:df:0d wlan0

7º – Agora deve-se criar um arquivo em uma pasta local. Este arquivo armazenará IV's (pacotes), o nome do arquivo foi chamado de *test* e sua extensão é .ivs. O comando anterior deverá continuar executando, portanto, deve-se abrir outro terminal e executar o comando a seguir:

 # airodump-ng -channel <Nº canal> --bssid <BSSID> --ivs –write <nomeArquivo> wlan0

8º – Por fim será foi executado o comando *aircrack-ng* que efetivamente efetuará a tentativa de quebra da criptografia WEP, também deverá ser aberto outro terminal para execução:

 # aircrack-ng -f 4 -n 128 test.ivs

// Observe-se que o nome do arquivo com os IV’s armazenados é chamado.

O resultado só foi possível graças ao armazenamento de um pouco mais de 65.000 pacotes em 4 dias de captura. A senha do ponto de acesso com endereço MAC ligado a ela (00:23:69:fa:9e:d1) é: arabin10grill. Na Figura 2 mostra o exemplo do momento do processo de captura de pacotes IV's:

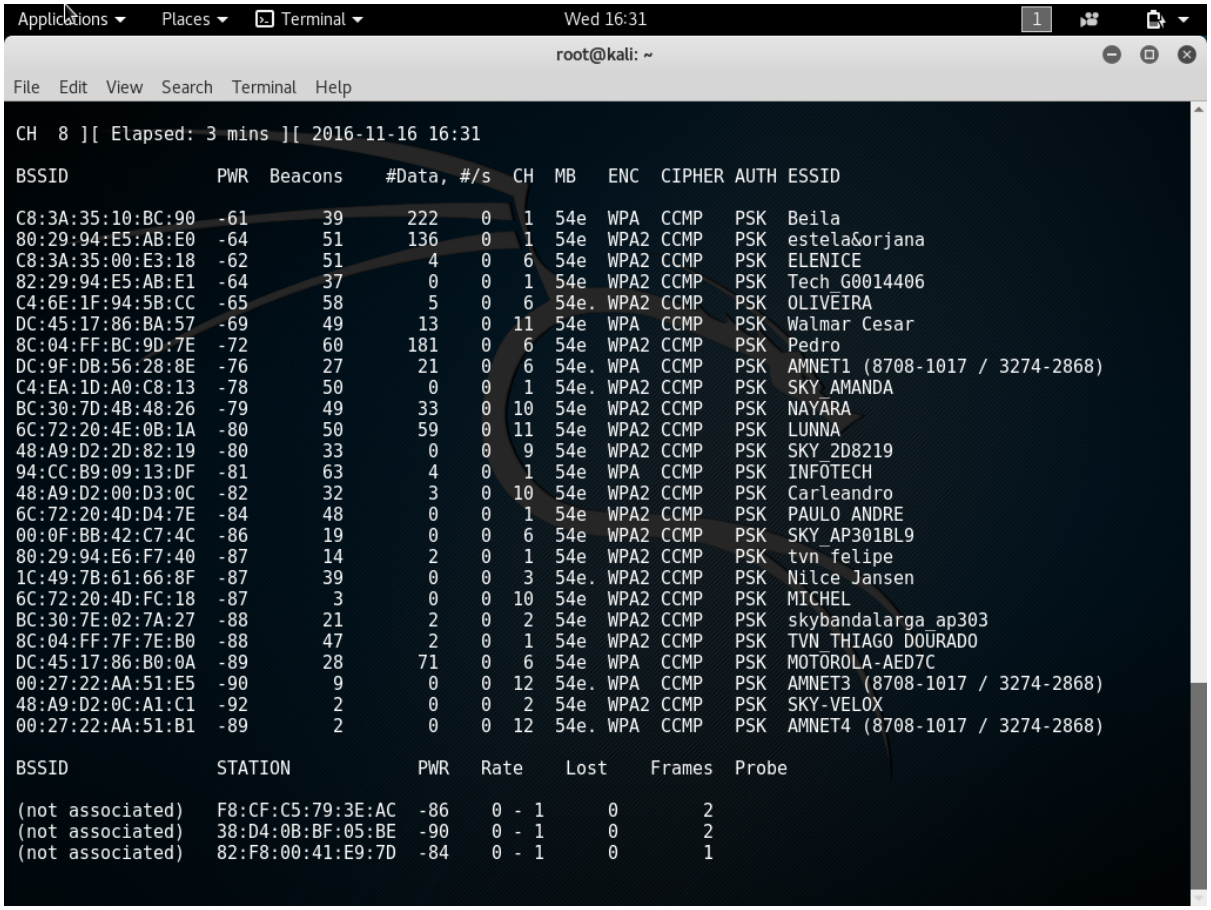

Figura 2 – Processo de captura de pacotes IV's

b) Tentativa de quebra da chave WAP no *shopping center* B.

O processo de quebra da chave WPA é parecido. Porém para a tecnologia de criptografia WPA é mais difícil de ser burlada. Para esta tarefa fez-se será necessário a utilização do ataque de força bruta que visam descobrir *passpharase*, baseadas em listas de dicionário, que podem ser encontradas fazendo a busca por "*wordlists*" no Google, também pode ser encontrado no repositório no seguinte endereço http://www.outpost9.com/files/WordLists.html. estas listas são armazenadas no diretório /usr/share/dict/words.

1º – Deverão ser seguidos os passos do tópico anterior para colocar a placa em modo monitor novamente. Isso serve para obter os dados da rede WPA e falsear um novo MAC para a placa *wireless* da maquina atacante.

2º – Abrir o terminal e executar o executar novamente o comando *airodump-ng* para capturar as transmissões, em outro terminal deverá rodar o *aireplay-ng* para desconectar o cliente e o obrigar a se reconectar ao ponto de acesso, de forma que os pacotes sejam capturados.

3º – Esse comando cria um arquivo chamado *lost.cap* onde serão armazenados os pacotes da rede do canal referenciado com o respectivo ponto de acesso.

 # airodump-ng -w lost –channel <nº canal> wlan0

4º – O comando a seguir irá simular uma solicitação de desconexão da maquina atacante ao ponto de acesso, desconectando o cliente especifico. O cliente certamente tentará se reconectar, fazendo com que a autenticação seja realizada novamente, neste momento os pacotes são capturados.

 # aireplay-ng -0 -1 -a <BSSID> -c <MAC falseado> wlan0

5º – Em outro terminal foi executada a tentativa de quebra de chave, usando a lista de palavras do diretório especificado anteriormente. Importa ressaltar que a *word list* possui mais de 5 Gigas de palavras chaves. Na decima terceira tentativa, houve sucesso.

 # aircrack-ng -e <SSID> -w /usr/share/dict/words lost.cap

Pode-se observar que esse processo só terá sucesso mediante a robustez da *wordlist*

versus ao nível de senha utilizada pelo ponto de acesso.

c) Tentativa de quebra da chave WPA2 no *shopping center* C.

O paradigma recente para quebra da criptografia WPA2 e principalmente o WPA2 diz que é extremamente demorado e difícil para serem quebrados. Entretanto, a recente técnica a ser utilizada para este experimento altera toda a visão sobre este paradigma.

Tudo mudou com o descobrimento de uma falha grosseira no protocolo WPS, que é suportado pela maioria dos roteadores atuais. Basicamente, o WPS oferece uma forma simples de configuração para as redes sem fio. O equipamento de acesso (*acess point*) inclui um PIN de 8 (oito) dígitos, geralmente informado em uma etiqueta na parte inferior, permitindo a conexão de qualquer cliente onde este PIN seja informado. A ideia do WPS é que seja um padrão de suporte para as redes domésticas.

> Desde o inicio, WPS parecia ser uma brecha esperando para ser explorada, mas a facilidade de configuração foi suficiente para reduzir bastante as chamadas de suporte e devoluções de produtos, o que foi suficiente para convencer quase todos os principais fabricantes a incluírem a tecnologia em seus roteadores domésticos. Eventualmente, a bomba explodiu, dando origem a maior brecha de segurança em redes *Wi-fi* desde o WEP. (MARIMOTO, 2012)

Ainda segundo Marimoto (2012):

> [...] a forma como o roteador responde as tentativas mal sucedidas de conexão, enviando um pacote WPA-NACK permite que o atacante descubra se os 4 primeiros dígitos do PIN estão corretos. Para piorar, o último digito do PIN é um *checksum*, que pode ser facilmente calculado uma vez que os 7 primeiros dígitos são conhecidos. Com isso, o atacante precisa de um número de tentativas suficiente para descobrir os 4 primeiros dígitos, gerar uma tabela com as possibilidades possíveis para os 3 últimos dígitos e mais o *checksum* (uma vez que o *checksum* é a soma dos 7 primeiros dígitos) e realizar uma última rodada de tentativas até encontrar o PIN correto. Com isso, o número de possibilidades cai de 1 bilhão para apenas 11.000 tentativas, que podem ser esgotadas em poucas horas.

O grande agravante para esse tipo de ataque é que uma vez que o consegue, em acesso à rede, continuará a conseguir conectar-se, mesmo que o administrador altere a chave de acesso ou mesmo o SSID da rede, seja ela WPA ou WPA2.

Para essa etapa de quebra de criptografia WPA2, foi utilizada a ferramenta Reaver. Seguem os passos utilizados:

1º – Para utilizar a ferramenta Reaver foi necessário colocar a placa em modo monitor. Para tal, abriu-se o *Kismet*. Se o *Kismet* não estiver executando automaticamente a placa de rede em modo de monitoramento (também conhecido como promíscuo), será faz-se necessário executar o comando para colocá-la em modo monitor:

airmon-ng start wlan0

// caso o comando anterior não seja executado, é porque o *Kismet* já está executando a placa em modo de monitoramento.

2º – O próximo passo é necessário foi obter informações sobre o dispositivo de rede e do endereço MAC do roteador alvo; para tal basta retirar as informações fornecidas pelo *Kismet*.

3º – Depois de descoberto o endereço MAC do ponto de acesso, o Reaver é executado no terminal, associando-o com MAC do ponto de acesso, com o seguinte comando:

 # reaver -i mon0 -b 97:FD:22:98:11:09 -vv

// onde o reaver = programar, mon0 = interface e 97:FD:22:98:11:09 = endereço MAC.

A partir deste ponto, todo o processo de ataque é realizado automaticamente, o

Reaver tenta todas as possibilidades possíveis para o PIN, até encontrar a chave PIN. A partir desta informação é possível ter acesso a rede WPA2. É importante ressaltar que por si só a criptografia WPA2 não é vulnerável.

3.2.2. Resultados – Pesquisa nos *shoppings*

Após a verificação e definição do nível de segurança dos protocolos de criptografias, foi aplicada a técnica *Wardriving* durante o período de 24 a 26 de outubro de 2016 com o objetivo de mapear as redes sem fio dos 5 grandes *shoppings* de São Luís – MA. Foram realizadas capturas externas de dentro de um carro, porém, como o sinal da antena não foi suficiente para fazer a cobertura de toda a área física do *shopping*, houve a necessidade da captura a partir das escolhas de pontos fixos internos dos *shoppings.*

3.2.2.1. Resultados – pesquisa *shopping center* A.

O *Shopping Center* A foi escolhido para coleta de dados por ser o maior da capital até 2 anos atrás e esperava-se encontrar um número significativo de redes sem fio protegidas. Foram identificados os nomes destas redes e os seus respectivos protocolos de criptografia. Como instrumento de trabalho utilizou-se um notebook com sistema operacional Kali Linux e ferramentas para levantamento de informações.

As capturas foram realizadas entre os dias 24 e 25 de outubro 2016 utilizando a técnica do *Wardriving* com captura externa dentro do carro e captura interna a partir da escolha de oito pontos fixos internos do *shopping*. Os locais foram escolhidos por serem pontos importantes para a cobertura de toda a área física. Após a escolha do local os dados foram coletados conforme mapeamento mostrado na Figura 3:

Figura 3 – Pontos de coletas *Shopping* A
FONTE: Google Maps (2017)

A linha em vermelha o compreende o caminho de deslocamento do carro para coleta das informações e as marcações em laranja representam os pontos fixos (visto de cima da parte externa do *shopping*) escolhidos para análise no *shopping* A.

A partir do caminho externo percorrido e dos oito pontos fixos, foi mapeado um total de 93 redes sem fio distintas encontradas pelo programa InSSIDer. Conforme ilustrado no gráfico 1 a seguir, do total de 93 redes sem fio localizadas, 13 estavam abertas para acesso, sem nenhum tipo de segurança. Sendo que, sua maioria (80) possuem algum tipo de protocolo de criptografia de segurança. Cabe ressaltar que 9 redes são possuidoras

do protocolo WEP que é 100% vulnerável a ataques. Assim sendo, 12 redes possuem o protocolo WPA e 59 do WPA2 que são detentoras de uma segurança mais avançadas, mas ainda vulnerável (dependendo das variáveis da infraestrutura utilizada em cada rede).

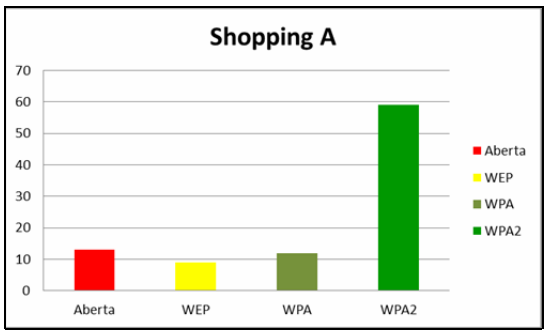

Gráfico 1 – Quantitativo das redes mapeadas no *Shopping* A.

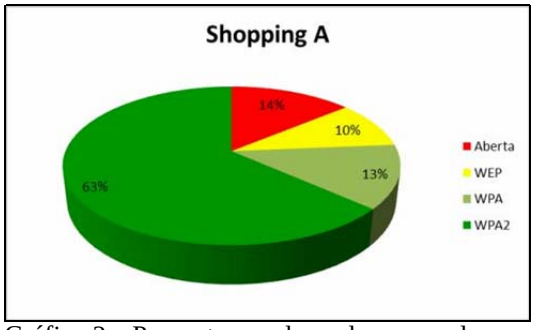

Gráfico 2 – Porcentagem das redes mapeadas no *Shopping* A.

O levantamento destes dados concretizada a partir da técnica do *Wardriving* foi para verificar o quantitativo das redes sem fio do *shopping* A e subdividir esse total em partes menores que compreendem o quantitativo das tecnologias de criptografia existente neste local. Através do gráfico 2, verificou-se que as redes que utilizam a tecnologia de criptografia WPA2 representam a grande maioria com 63% do total de redes, enquanto que redes com WPA possuem 13%, WEP 10% e redes abertas representam 14%.

3.2.2.2. Resultados – pesquisa *shopping center* B.

O *Shopping Center* B foi escolhido para coleta de dados por ser o maior *shopping* da capital do Estado do Maranhão e esperava-se um número pequeno de redes sem fio desprotegidas. Foram identificados os nomes destas redes e os seus protocolos de criptografia. As capturas foram realizadas entre os dias 24 e 25 de outubro utilizando a técnica do *Wardriving* com captura externa dentro do carro e captura interna a partir da escolha de doze pontos fixos do *shopping*, sendo seis no primeiro andar e mais seis no segundo. Os locais foram escolhidos por serem pontos importantes para a cobertura de toda a área física do *shopping*. Após a escolha do local os dados foram coletados conforme mapeamento mostrado na Figura 4:

Figura 4 – Pontos de coletas *Shopping* B
FONTE: Google Maps (2017)

A linha em vermelho corresponde ao caminho de deslocamento do carro para coleta das informações e as marcações em laranja representam os pontos fixos (visto de cima da parte externa do *shopping*) escolhidos para análise no *shopping* B. A partir do caminho externo percorrido e dos doze pontos fixos foram identificadas um total de 135 redes sem fio distintas. Destas 135 redes localizadas, 14 estavam abertas, sem nenhum tipo de segurança. Sua maioria (121 das 135) possui algum protocolo de criptografia de segurança. Cabe ressaltar que 22 possuidoras do protocolo WEP são vulneráveis a ataques. Assim sendo, 21 redes possuem o protocolo WPA e 78 do WPA2.

A seguir o gráficos 3:

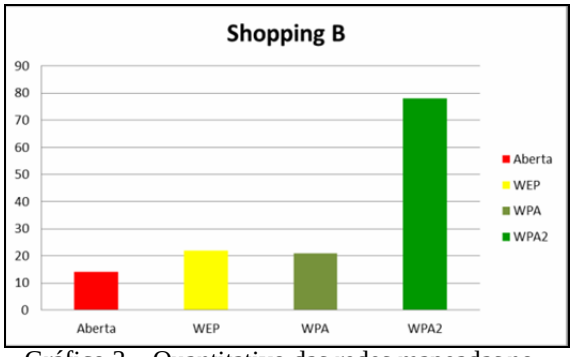

Gráfico 3 – Quantitativo das redes mapeadas no *Shopping* B.

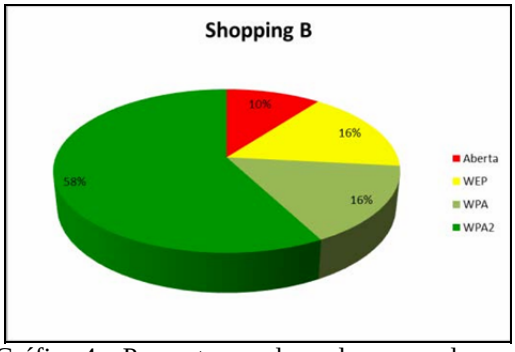

Gráfico 4 – Porcentagem das redes mapeadas no *Shopping* B.

A partir dos dados mostrados no gráfico 4, foi possível verificar a porcentagem dos protocolos de criptografia utilizados no *shopping* B. Verificou-se que as redes que utilizam a tecnologia de criptografia WPA2 representam 58% do total geral de redes, enquanto que redes com criptografia WEP e WPA representam ambas respectivamente 16%, 10% são referentes as redes abertas ou sem nenhum tipo de proteção.

3.2.2.4. Resultados – pesquisa *shopping center* C.

O *Shopping Center* C foi escolhido para coleta de dados por ser o *shopping* localizado mais próximo da periferia da capital maranhense, tendo um ótimo fluxo de pessoas, porém, com um número de lojas reduzidas. Esperava-se encontrar um número pequeno de redes sem fio. As capturas foram realizadas no dia 26 de maio com captura externa dentro do carro e captura interna a partir da escolha de seis pontos fixos do *shopping*. Os locais foram escolhidos por serem pontos importantes para a cobertura de toda a área física do *shopping*. Após a escolha do local os dados foram coletados conforme mapeamento mostrado na Figura 5:

Figura 5 – Pontos de coletas *Shopping* C
FONTE: Google Maps (2017)

A linha em vermelho compreende o caminho de deslocamento do carro para coleta das informações e as marcações em laranja representam os pontos fixos (visto de cima da parte externa do *shopping*) escolhidos para análise no *shopping* C.

A partir do caminho externo percorrido e dos seis pontos fixos foram obtidos um total de 72 redes sem fio distintas encontradas pelo programa de captura de informações, o InSSIDer. Destas 72 redes localizadas, 9 estavam abertas, sem nenhum tipo de segurança. Sendo que, em sua maioria (63 das 72) possuem algum tipo de protocolo de criptografia. Em relação às redes que utilizam o protocolo WEP, 16 foram identificadas com este tipo de criptografia. Assim sendo, 12 redes possuem o protocolo WPA e 35 são do tipo WPA2. Esse quantitativo é apresentado no gráfico 5.

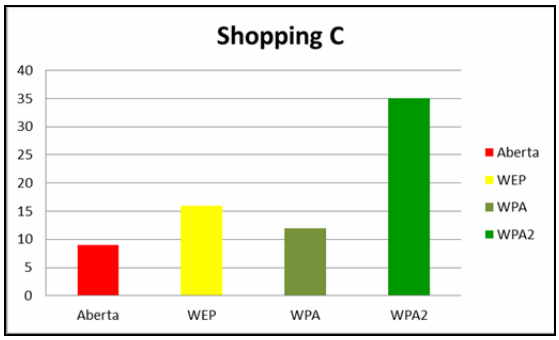

Gráfico 5 – Quantitativo das redes mapeadas no *Shopping* C.

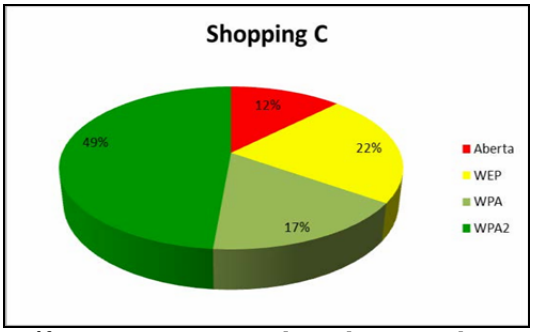

Gráfico 6 – Porcentagem das redes mapeadas no *Shopping* C.

A partir dos dados mostrados no gráfico 6, foi possível verificar a porcentagem dos protocolos de criptografia utilizados no *shopping* C. Verificou-se que as redes que utilizam a tecnologia de criptografia WPA2, possuem menos da metade do quantitativo geral em relação as demais juntas, representando 49% do total de redes. Enquanto que redes com criptografia WPA representam 17%, tendo as redes com tecnologia WEP com 22% e 12% referentes às redes abertas.

3.2.2.5. Resultados – pesquisa *shopping center* D.

O *Shopping Center* D foi escolhido para coleta de dados por ser o *shopping* localizado próximo da área nobre capital maranhense, tendo um grande fluxo de pessoas, com um grande número de lojas. Esperava-se encontrar uma grande quantidade de redes sem fio. Foram identificados os nomes destas redes e os seus protocolos de criptografia. Vale a pena ressaltar que na verdade são dois *shopping*s compartilhando a mesma clientela. Por conta do objetivo maior da pesquisa, estes dois serão considerados como um único ambiente.

As capturas foram realizadas entre os dias 25 e 26 de outubro com captura externa dentro do carro e captura interna a partir da escolha de dez pontos fixos (4 no *shopping* de andares e 6 no do *shopping* com lojas no térreo). Os locais foram escolhidos por serem pontos importantes para a cobertura de toda a área física do *shopping*. Após a escolha do local os dados foram coletados conforme mapeamento mostrado na Figura 6:

Figura 6 – Pontos de coletas *Shopping* D
FONTE: Google Maps (2017)

A linha em vermelho compreende o caminho de deslocamento do carro para coleta das informações e as marcações em laranja representam os pontos fixos internos escolhidos para análise no *shopping* D. A partir do caminho externo percorrido e dos dez pontos fixos foram obtidos um total de 177 redes distintas encontradas pelo programa utilizado para captura de informações. Destas 177 redes, 18 estavam abertas, sem nenhum tipo de segurança. Sendo que, em sua maioria (159 de 177) possuem algum tipo de criptografia. Destas 159 que possuem proteção, 25 são possuidoras do protocolo de criptografia WEP, outras 20 redes possuem o protocolo WPA e 114 são do tipo WPA2.

No gráfico 7 é apresentado este quantitativo:

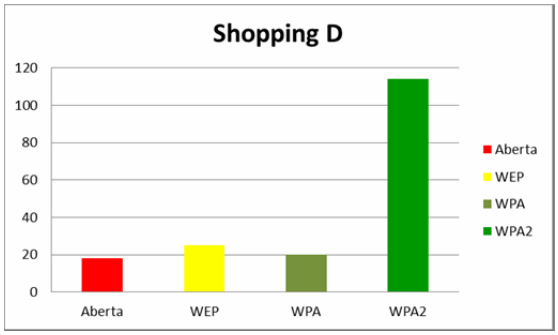

Gráfico 7 – Quantitativo das redes mapeadas no *Shopping* D.

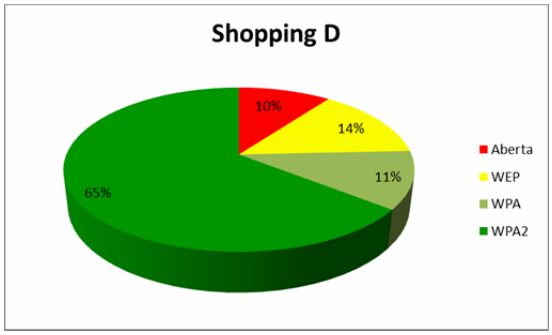

Gráfico 8 – Porcentagem das redes mapeadas no *Shopping* D.

O gráfico 8 apresenta a divisão em porcentagens das redes sem fio e suas respectivas tecnologias de criptografia encontradas no *shopping* D. Verificou-se que as redes que utilizam a tecnologia de criptografia WPA2 representam a grande maioria com 65% do total de redes, enquanto que redes com WPA possuem 11%, WEP 14% e as redes abertas representam 10%.

3.2.2.6. Resultados – pesquisa *shopping center* E.

O *Shopping Center* E foi escolhido para coleta de dados por ser o *shopping* intermediário localizado próximo do *shopping* A e D. Esperava-se encontrar um número razoável de redes sem fio. As capturas foram realizadas entre no dia 26 de outubro utilizando a técnica do *Wardriving* com captura externa dentro do carro e captura interna a partir da

escolha de quatro pontos fixos internos do *shopping*. Após a escolha dos locais os dados foram coletados conforme mapeamento mostrado na Figura 7:

Figura 7 – Pontos de coletas *Shopping* E
FONTE: Google Maps (2017)

A linha em vermelha compreende o caminho de deslocamento do carro para coleta das informações e as marcações em laranja representam os pontos fixos (visto de cima da parte externa do *shopping*) escolhidos para análise no *shopping* E.

A partir do caminho externo percorrido e dos quatro pontos fixos, foram obtido um total de 56 redes distintas. Destas 56, apenas 13 estavam abertas, sem nenhum tipo de segurança. Sendo que, sua maioria (43 das 56 encontradas) utilizavam de algum tipo de protocolo de criptografia. Cabe ressaltar que apenas 6 são possuidoras do protocolo WEP. Assim sendo, 10 redes possuem o protocolo WPA e 27 utilizam o protocolo WPA2.

No gráfico 9 é apresentado estes valores em escala:

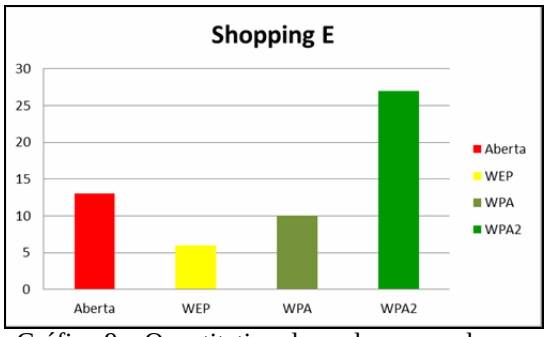

Gráfico 9 – Quantitativo das redes mapeadas no *Shopping* E.

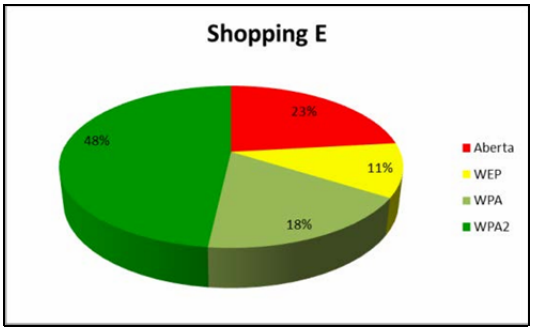

Figura 10 – Porcentagens das redes mapeadas no *Shopping* E.

Conforme mostrado no gráfico 10, verificou-se que as redes, que utilizam a tecnologia de criptografia WPA2, representam 48% do total de redes, enquanto que redes com WPA possuem cerca de 18%, a WEP com apenas 11% e as redes abertas representam 23% do total.

3.3. Discussão

> Implementações de novas tecnologias sem fio e sem a prévia análise podem resultar em sérios riscos, podendo gerar impactos negativos que contrapõem e até mesmo anulam os benefícios alcançados, seja por não se incorporarem adequadamente aos sistemas de informações que os suportam, seja por trazerem consigo outras falhas inesperadas, por vezes maiores que as falhas que uma tecnologia possa vir a corrigir. (SCHNEIER, 2009, p. 83)

Efetuando a análise dos dados obtidos, constata-se que existe certa variação na utilização dos diferentes tipos de tecnologias de criptografia. Para fins didáticos são criados dois agrupamentos distintos a fim de consolidar os resultados. O primeiro é constituído pelo quantitativo de redes com criptografia WPA2 e WPA e o segundo com a tecnologia WEP e redes abertas. Tal divisão parte do pressuposto de que as redes utilizam WPA2 e WPA são mais difíceis de serem quebradas do que a WEP que é 100% vulnerável. Considerando a classificação dos *shopping*s baseando-se na quantidade total das redes encontradas nas mesmas, tem-se o seguinte ranking: 1º *Shopping* D (177), 2º *Shopping* B (135), 3º *Shopping* A (93), 4º *Shopping* C (72), 5º *Shopping* E (56).

No *shopping center* A, a relevância da porcentagem obtida dos protocolos de criptografia WPA2 e WPA, é satisfatória. Apresentam juntas cerca de 76% do total das redes que utilizam este tipo de criptografia, que atualmente são as mais seguras. *No shopping center* B, verifica-se que existe mais da metade de redes com algum tipo de criptografia de dados, essa grande maioria são de pontos de acesso que utilizam WPA2, com 58%. Somada as redes que utilizam a criptografia WPA (16%) os números totais das mesmas chegam a 73%.

Analisando os dados fornecidos no capitulo anterior, verifica-se no *shopping* C 34% das redes ou estão abertas para acesso livre ou utilizam criptografia WEP, essa quantidade é considerada alta. Observa-se também que o quantitativo das redes com WPA2 não passa da metade do total geral, que é considerado um fator critico para um ambiente com alto índice de usuários. No *shopping center* D, verifica-se que existe mais da metade de redes com algum tipo de criptografia de dados, essa grande maioria são de pontos de acesso que utilizam WPA2 (64%) e WPA (11%). Somando estes valores o total é de 76% (em números representa 134 redes).

Cumpre ressaltar que, dos 5 *shoppings* onde esta pesquisa foi realizada, o *shopping* D apresentou a maior quantidade de redes protegidas com algum tipo de protocolo de criptografia. Levando-se em consideração os resultados obtidos no *shopping* E, neste caso especifico, o quantitativo de redes abertas e que utilizam sistema WEP de criptografia de dados, representam juntas 34% do total. Então, pode-se afirmar que este ambiente possui um nível de segurança ruim, pois possui mais de 30% de vulnerabilidade. Na Tabela 3, apresenta-se o resultado final obtido através dos estudos realizados:

Alguns pesquisadores dizem que as principais aplicações estão rodando sobre os protocolos SSL (*Secure Socket Layer*) e TLS (*Transport Layer Security*) que permite (permitia) a integridade e confidencialidade dos dados que são passados entre o cliente e o servidor. Entretanto em 2011 pesquisadores tailandeses Thai Duong e Juliano Rizzo conseguiram pela primeira vez quebrar estes protocolos, utilizando *exploit* programado em JavaScript que funciona como um farejador de rede (*sniffer),* tendo a capacidade de decifrar a informação. Tal informação reforça a tese que uma vez que a rede sem fio é aberta, não significa dizer que as aplicações que utilizam outros protocolos de segurança como o SSL/TLS são totalmente confiáveis.

Local	Criptografia	Quantidade	Porcentagem	Total	Nivel de Vulnerabilidade
Shopping A	WPA2	59	63	93	Vulnerabilidade Baixa
	WPA	12	13		
	WEP	9	10		
	Aberta	13	14		
Shopping B	WPA2	78	58	135	Vulnerabilidade Baixa
	WPA	21	16		
	WEP	22	16		
	Aberta	14	10		
Shopping C	WPA2	35	49	72	Vulnerabilidade Alta
	WPA	12	17		
	WEP	16	22		
	Aberta	9	13		
Shopping D	WPA2	114	64	177	Vulnerabilidade Baixa
	WPA	20	11		
	WEP	25	14		
	Aberta	18	10		
Shopping E	WPA2	27	48	56	Vulnerabilidade Alta
	WPA	10	18		
	WEP	6	11		
	Aberta	13	23		

Tabela 3 - Resultados finais

4. CONCLUSÃO

Esta pesquisa procurou expressar um cenário onde o fator de vulnerabilidades nas redes sem fio nos ambientes públicos (*shoppings*) podem ser um fator critico para o aumento do roubo de informações. O trabalho também procurou abordar por meio da contextualização e pesquisa aplicada, identificar às vulnerabilidades as redes sem fio e suas criptografias de maneira a demonstrar e esclarecer como funciona este modelo de ataque e os seus impactos, além da importância da necessidade de proteção.

Inicialmente, por meio do estudo bibliográfico, foram esclarecidos os conceitos da segurança da informação, das redes sem fio e os mecanismos de segurança que envolvem as mesmas. Posteriormente, a partir dos resultados obtidos, foram apresentadas as facilidades peculiares que propiciam a atuação do atacante no processo de invasão das redes sem fio, que atuam na grande maioria das vezes de forma indireta, sem a necessidade de presença física nos locais alvos. O crescimento descentralizado e constante das redes sem fio esta relacionado aos impactos das exposições de informações dos usuários é uma constante que deve ser estuda, combatida e acompanhada com mais veemência nos campos computacionais.

Foi visto que, em São Luís, no total de 533 redes sem fio, mapeadas durante a utilização da técnica do *wardriving* na identificação das redes sem fio nos *shoppings* da capital maranhense, 313 redes utilizam criptografia WPA2, que representa 59% do total geral, ou seja, uma quantidade elevada. Pode-se concluir que, apesar de 2 *shoppings* terem quantidades altas de redes abertas e que utilizam criptografia WEP, nada impacta o resultado final geral, ou seja, baseando-se apenas no total das redes com WPA2 (redes mais seguras) e WPA o saldo geral no que refere-se a segurança da informação das redes sem fio na capital maranhense é caracterizado como :"BOM". Entretanto, percebe-se também, a necessidade de ampliação ou criação do número de equipes capazes de trabalhar com a gestão da Segurança da Informação nas empresas e órgãos públicos, profissionais estes capazes de treinar a sua equipe e ter respostas a incidentes eficazes.

Também foram apresentadas, à qualidade do tratamento das informações e construção de uma infraestrutura de rede mais confiável. Algumas medidas importantes citadas para aumentar a segurança em redes sem fio são: ler o manual de uso do

equipamento inteiro durante a primeira instalação para habilitar o tipo de protocolo de criptografia (evite deixar sem senha ou utilizar o tipo WEP); cadastrar os endereços das maquinas clientes (*MAC ADRESS*) fixas que utilizaram a rede, desabilite/oculte a visualização da rede para visitantes (o *broadcast de SSID)*; desligar o ponto de acesso quando não estiver em uso; limitar o acesso a números de máquinas pré- definidas e trocar com frequência a senha de acesso a rede sem fio. Outro aspecto relevante o qual merece ser dada a devida atenção é o papel do Estado Brasileiro na divulgação e implantação de políticas profundas que levem em consideração as bases da segurança da informação.

Conclui-se, portanto, que a pesquisa desenvolvida obteve êxito no seu papel maior que é conscientizar a sociedade para os riscos em que estão envolvidos os usuários das redes sem fio em locais públicos.

REFERÊNCIAS BIBLIOGRÁFICAS

ALVES, G. A. Segurança da Informação: uma visão inovadora da gestão. São Paulo: Ifweb, 2010.

BBC. Para especialista americano espionagem do Brasil não se compara à da NSA. 2013. Disponível em: < > Acesso em: 11 nov. 2013.

GIL, A. C. Como elaborar projetos de pesquisa. 4 ed. São Paulo: Atlas, 2010.

HURLEY, P. M.; FAIRBAIRN, H. W. System Networks Attacks. 1978. Geal, Sco. Am. Bull 89.

LUCCHESE, F. Utilizando *Wardriving* para a detecção de vulnerabilidades em redes locais sem fio na região Farroupilha. Novo Hamburgo: 2007

GOOGLE MAPS. (2013). Disponivel em <https://maps.google.com.br> Acesso em: 16 nov. 2013.

MARTINS, G. Análise de vulnerabilidades e ataques a redes sem fio 802.11. São Paulo: Informática, 2012.

MARIMOTO, C. E. Hardware, o guia definitivo. Porto Alegre: Sul Editores, 2009.
.
OSM, Open Street Map, São Luís, 2013. Disponível em: <> Acesso em: 11 de nov. 2013.

PEIXOTO, M. C. P. KONSULTEX. Rio de Janeiro: Braspost, 2008.

RUFINO, N. Segurança em Redes sem Fio. 2 ed. São Paulo: Novatez, 2010.

SCHNEIER, B. Segurança.com: Segredos e Mentiras sobre a Proteção na Vida Digital. São Paulo: 2001.