Segurança em Redes *Wireless* Domésticas: Um Estudo de Caso

Izabella Xavier, Pedro Oliveira, Alex Feleol

Fundação Centro de Análise, Pesquisa e Inovação Tecnológica – FUCAPI

CEP 69075-351 – Manaus – AM – Brazil

{izabellatello, peoliveira@gmail.com, alex@sec4all.com.br}

Abstract. *This article describes a case study, whose objective is to demonstrate the necessity of best practices in information security applied to domestic wireless networks, through analysis of vulnerabilities in wireless networks found in a residential complex in the city of Manaus, in which, procedures of pentest and use of support tools were based on the methodology PTES (Penetration Testing Execution Standard), including enabling the correction of vulnerabilities found, when it is authorized.*

Resumo. *Este artigo descreve um estudo de caso, cujo objetivo é demonstrar a necessidade de boas práticas em segurança da informação aplicadas às redes wireless domésticas, através da análise de vulnerabilidades em redes wireless encontradas em um conjunto residencial na cidade de Manaus, na qual, os procedimentos de pentest e utilização das ferramentas de apoio tiveram como base a metodologia PTES (Penetration Testing Execution Standard), inclusive possibilitando a correção das vulnerabilidades encontradas, quando autorizadas.*

1. Introdução

Com a constante expansão da Internet, a popularidade das redes *wireless* cresce de forma significativa associada às facilidades oriundas desta tecnologia aos dispositivos móveis. Diante disso, há uma diminuição direta no custo de equipamentos necessários a esse tipo de tecnologia, ocasionando, ainda, a facilidade e a comodidade relacionadas à aquisição e à utilização dos mesmos [FLICKENGER et al., 2008].

De acordo com dados do Comitê Gestor da Internet no Brasil (2013), em 2012, verificou-se que 74% dos usuários acessam a Internet de redes domésticas, equivalente ao crescimento de seis pontos percentuais sobre 2011 e trinta e dois pontos sobre 2008.

Considerando as possíveis vulnerabilidades dos equipamentos necessários para uma rede *wireless* relacionadas à má configuração executada por usuários leigos, este estudo de caso foi desenvolvido em um conjunto residencial, localizado na cidade de Manaus, onde este perfil de usuário pode ser encontrado com relativa facilidade. Tem como objetivo demonstrar a necessidade de implementação de medidas de segurança em redes *wireless* domésticas, visando diminuir possíveis vulnerabilidades inerentes a esse tipo de tecnologia ao utilizar boas práticas de segurança da informação.

Com base neste cenário, foram realizados testes de intrusão, originalmente conhecidos como *pentests*, associados às ferramentas de análise e com o objetivo de avaliar a segurança adotada para cada rede *wireless*.

Este artigo está organizado em mais quatro seções. Na seção 2, denominada "Metodologia", são abordadas as metodologias PTES e *WLAN Penetration Testing Methodology*, associadas às ferramentas de análise à intrusão. Na seção 3, "Estudo de Caso", há a descrição do cenário com a aplicação das ferramentas utilizadas para realização do *pentest*, desde o processo de captura de pacotes das redes (para delimitação do escopo) até os resultados obtidos nos testes de intrusão. A seção 4 apresenta os resultados obtidos e as medidas de segurança sugeridas mediante cada tipo de ataque bem-sucedido, além da conscientização aplicada aos usuários das redes com base nas boas práticas de segurança. As conclusões e perspectivas são abordadas na seção 5.

2. Metodologia

Nesta seção pretende-se apresentar as metodologias utilizadas para o desenvolvimento do estudo de caso e as ferramentas complementares utilizadas.

2.1. *PTES*

O PTES (*Penetration Testing Execution Standard*) é uma metodologia utilizada para a realização de testes de intrusão com o intuito de padronizar e aumentar a qualidade desse tipo de atividade [PTES *Technical Guidelines*, 2012]. Esse padrão inclui sete seções que definem o conteúdo e as sugestões apresentadas, desde a formalização legal até os relatórios finais.

As principais fases aplicadas neste estudo de caso são:

- *Pre-engagement Interactions:* acordam-se os documentos legais e definem-se as especificidades do escopo;
- *Intelligence Gathering:* detalham-se e coletam-se as informações necessárias para as operações a serem realizadas;
- *Threat Modeling:* com base nas informações coletadas na fase anterior, realiza-se uma modelagem das ameaças e seus elementos encontrados para auxiliar a análise posterior;
- *Vulnerability Analysis*: descrevem-se as principais áreas em que a análise de vulnerabilidades deve cobrir conforme os resultados anteriores;
- *Exploitation:* executam-se os ataques de intrusão conforme as vulnerabilidades elucidadas na fase anterior;
- *Reporting*: apresenta-se o relatório conclusivo das atividades.

Essa metodologia é aplicada comumente em empresas e organizações, porém foi adaptada de acordo com o cenário desse estudo de caso.

2.2. Metodologia de Testes de Intrusão em WLAN

Denominada em inglês como *WLAN Penetration Testing Methodology*, essa metodologia foi aplicada neste estudo de caso em complemento ao PTES. Conforme afirma Ramachandran (2011), esta metodologia de teste de intrusão divide-se em quatro fases: Planejamento, Descoberta, Ataque e Relatório.

Na fase de Planejamento, é definido o escopo com informações como área de cobertura dos testes e quais redes estão incluídas na avaliação. Além disso, é estimado o esforço a ser gasto, com definições do número de dias disponíveis e a profundidade dos requisitos bases para os testes. Nesta fase também se enfatiza a parte referente aos acordos de não divulgação dos dados. Após as definições anteriores, realiza-se uma varredura das redes sem fio da área, chamada de fase de Descoberta.

Encontrar pontos de acesso, quebrar criptografias e invadir infraestruturas são as subfases da etapa de Ataque. Nesta fase recomenda-se a utilização de ferramentas como *Airodump-ng* e *Aircrack-ng*. Ao final, após elucidar as vulnerabilidades, faz-se necessário relatá-las, na chamada fase Relatório, onde cada teste de intrusão deve ter informações específicas como: descrição da vulnerabilidade, gravidade, tipo de vulnerabilidade – software/hardware/configuração, soluções alternativas e sugestões de remediação.

2.3. Ferramentas de Apoio e Análise

O Quadro 1 contém a lista com as ferramentas utilizadas neste estudo de caso, com suas respectivas versões e funções.

Quadro 1. Descritivo das ferramentas de apoio utilizadas

Ferramentas	Versão	Utilização
Vistumbler	10.3	Efetua a varredura do ambiente local em busca de redes *wireless.*
Wifi Analyzer	3.6.5	Efetua a medição da intensidade de sinal das redes *wireless.*
Wifite	2 (r85)	Efetua a varredura das redes *wireless* com WPS habilitado.
Reaver	1.3	Efetua ataques às redes *wireless* com WPS habilitado.
Airodump-ng	1.2	Coleta informações sobre as redes *wireless.*
Airmon-ng	1.2	Ativa o modo de monitoramento promíscuo da placa de rede.
Airbase-ng	1.2	Acelera o processo de captura de dados (requisição ARP e autenticações falsas).
Aircrack-ng	1.2	Efetua a decodificação de senhas em dados capturados.
Aireplay-ng	1.2	Cria um ponto de acesso falso, mais conhecido como *Honeypot.*
Wireshark	1.1.0.2	Efetua a análise de tráfego de rede (*sniffer*).

2.4. Dicionário de Senhas

É comum fabricantes utilizarem senhas curtas, acreditando que ao instalar e configurar seu ponto de acesso, o usuário irá modificar a senha [RUFINO, 2011]. Diante disso, Wilhelm (2010) afirma que a decodificação de senhas é uma das principais partes dos testes de penetração, portanto acredita-se que a melhor forma é criar o próprio dicionário de senhas conforme o cenário de atuação.

2.5. Engenharia Social

Wilhelm (2010) também destaca a utilização de ataques de Engenharia Social, afirmando que este tipo de ataque é extremamente eficaz, no caso de redes, a pessoa normalmente quer ser útil e acaba fornecendo a informação. É por este fato que é necessário instruir ou treinar as pessoas sobre esse assunto pra impedir esse tipo de ataque.

2.6. Verificações da Eficácia

A CERT.br é o Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil, desde 1997. Além de ser o responsável por tratar incidentes de segurança, também desenvolve análise de tendências, treinamento e conscientização.

Por conta da abrangência e linguagem utilizada por essa organização, destacaram-se as boas práticas aplicadas aos cuidados ao montar uma rede *wireless* doméstica. De acordo com a CERT.br (2012), para um bom funcionamento e segurança de uma rede doméstica, deve-se fazer principalmente:

- Alterar configurações padrões, como por exemplo, senhas (de administração e do próprio Ponto de Acesso);
- Utilizar senhas bem elaboradas e difíceis (que não contenham informações pessoais como sobrenome e datas de nascimento, por exemplo);
- Desativar a opção WEP e utilizar WPA2 ou no mínimo WPA;
- Desligar o Ponto de Acesso quando não estiver usando a rede;
- Desabilitar a difusão do SSID (*broadcast*) para evitar que o nome da rede seja visualizado por outros dispositivos;
- Ao definir o SSID, não utilizar dados pessoais e nomes associados ao fabricante e/ou modelo do Ponto de Acesso, por exemplo;
- Desabilitar a opção de WPS (*Wi-fi Protected Setup*), caso o Ponto de Acesso disponibilize-a;

2.7. Trabalhos Relacionados

Observou-se que há uma série de trabalhos e publicações que proporcionam informações relacionadas às diversas seções deste assunto. Dentre estes, foram selecionados os trabalhos a seguir com o intuito de enriquecer este artigo:

O artigo publicado por Moreira *et al.* (2011), intitulado “Avaliação de segurança em redes sem fio”, aborda uma avaliação do nível de segurança dos protocolos WEP, WPA e WPA2, através de ataques com ferramentas como o *Aircrack-ng*, *Airmon-ng* e *Aireplay-ng*. Após as avaliações, o estudo concluiu que os protocolos WEP e WPA são inseguros e complementou que o WPA2 com o PSK criptografado com o AES é a melhor recomendação de configuração no momento.

O segundo trabalho relacionado trata-se de um artigo intitulado “Boas práticas de segurança para redes domésticas: instalação e configuração de ativos para torná-las seguras”, no qual Serique Junior *et al.* (2012) realiza um estudo de caso sobre o risco da construção de rede doméstica quando instalada em modo padrão, verificando que medidas corretivas, como por exemplo configuração adequada de roteadores, podem minimizar significativamente as vulnerabilidades e os riscos oferecidos por uma rede doméstica sem o devido tratamento de segurança.

Em “Vulnerabilidade da Segurança em Redes Sem Fio**”,** Pinzon (2009), ao analisar vulnerabilidade em alguns pontos de rede *wi-fi* existentes na cidade de Porto Alegre, conclui que as técnicas de segurança necessitam de conhecimento e gerar um padrão de segurança torna-se imprescindível para este tipo de tecnologia.

Horovits (2013), em seu trabalho intitulado “Explorando vulnerabilidades em redes sem fio: usando as principais ferramentas de ataque e configurações de defesa”, demonstra como configurar um roteador para conter uma segurança maior em uma rede

sem fio e conclui que se deve ter uma maior atenção nesse quesito, pois há várias formas de ataques para quebrar as criptografias existentes.

3. Estudo de Caso

Este artigo consiste em um estudo de caso exploratório de redes *wireless* domésticas, localizadas em um conjunto residencial de Manaus, que por razões de privacidade seus nomes serão omitidos.

3.1. Cenário

O escopo definido para este cenário possui onze redes *wireless* domésticas, cujas configurações não sofreram qualquer influência prévia deste trabalho. As redes foram selecionadas a partir de um ponto fixo como marco base para as demais, ou seja, foi definido um local de uma das casas do conjunto escolhido e, com a ajuda do *software Vistumbler*, as redes que foram detectadas, independente da potência de seu sinal, foram delimitadas para o escopo a ser analisado. Neste cenário foram encontradas criptografias WEP, WPA e WPA2, conforme mostra a Figura 1:

#	Active	Mac Address	SSID	Signal	High Signal	RSSI	High RSSI	Channel	Authentication	Encryption
1	Active	00:25:9C:20:F9:39	[illegible]	89%	89%	-58 dBm	-48 dBm	6	WPA2-PSK	AES
2	Active	D8:5D:4C:CE:EA:4E	[illegible]	36%	60%	-72 dBm	-68 dBm	11	WPA2-PSK	AES
3	Active	64:66:B3:87:56:63	[illegible]	28%	38%	-76 dBm	-71 dBm	11	WPA2-PSK	AES
4	Active	94:CC:D9:88:FB:DD	[illegible]	10%	20%	-85 dBm	-80 dBm	1	WPA-PSK	AES
5	Active	B0:48:7A:D4:83:BA	[illegible]	16%	26%	-82 dBm	-77 dBm	3	WPA2-PSK	AES
6	Active	00:23:69:BC:A8:F3	[illegible]	86%	90%	-49 dBm	-44 dBm	6	Open	WEP
7	Active	00:18:E7:CF:2C:C0	[illegible]	12%	24%	-84 dBm	-78 dBm	6	WPA2-PSK	AES
8	Active	F0:7D:68:E2:45:B8	[illegible]	18%	30%	-81 dBm	-75 dBm	6	WPA2-PSK	AES
9	Active	00:23:CD:D3:09:C4	[illegible]	22%	32%	-79 dBm	-74 dBm	6	WPA2-PSK	AES
10	Active	D8:5D:4C:EA:77:4C	[illegible]	16%	22%	-82 dBm	-79 dBm	8	WPA2-PSK	AES
11	Active	74:EA:3A:A7:68:B4	[illegible]	70%	81%	-63 dBm	-56 dBm	4	WPA2-PSK	AES

Figura 1. Lista das redes wireless encontradas

3.2. Coleta de Informações

Após a delimitação do escopo, foi realizada a atividade de coleta das autorizações, de cada proprietário das respectivas redes, para testes de vulnerabilidades. Na autorização, o proprietário informa ainda se permite que as melhorias propostas sejam realizadas e se deseja responder ao questionário complementar.

O questionário complementar engloba perguntas diretas (com respostas Sim/Não), conforme mostra a Tabela 1, sobre o conhecimento técnico em informática, seja das pessoas que residem na casa ou da pessoa que configurou o roteador, além de confirmar se há crianças e se há outros tipos de dispositivos conectados à rede da casa. O proprietário também é questionado sobre a preocupação quanto à definição de suas senhas de rede.

O intuito do questionário é direcionar as informações, de forma simplória, a serem esclarecidas na etapa de aplicação das melhorias. É um auxílio para a definição de qual tipo de cartilha será entregue aos usuários de cada rede conforme a delimitação do escopo. Além de embasar a principal motivação deste trabalho: a ausência de precauções quanto à segurança de redes *wireless* domésticas.

Tabela 1. Resumo do questionário complementar

N.º	**PERGUNTA (S – Sim / N – Não)**	**WiFi 01**	**WiFi 02**	**WiFi 03**	**WiFi 04**	**WiFi 05**	**WiFi 06**	**WiFi 07**	**WiFi 08**	**WiFi 09**	**WiFi 10**	**WiFi 11**	**Total (S – Sim)**	**Percentual (S – Sim)**
1	Há crianças?	S	S	S	S	S	N	N	S	N	S	N	**7**	**64%**

2	Há outros dispositivos (celulares, tablets, etc) conectados na rede além de computadores?	S	S	S	S	S	S	S	S	S	S	S	**11**	**100%**
3	Há alguém que tenha conhecimento técnico sobre informática?	S	S	N	N	N	N	N	N	N	S	N	**3**	**27%**
4	O responsável pela configuração do roteador possui conhecimento técnico sobre informática?	N	N	S	S	N	N	N	N	N	S	N	**3**	**27%**
5	Há algum tipo de manutenção no roteador (atualizações, por exemplo)?	N	N	N	N	N	N	N	N	N	S	N	**1**	**9%**
6	Pessoa que realiza esta atividade possui conhecimento técnico sobre informática?	N	N	N	N	N	N	N	N	N	S	N	**1**	**9%**
7	Já teve algum conhecimento de alguma invasão à sua rede?	N	N	N	N	N	N	N	N	N	N	N	**0**	**0%**
8	Você sabe verificar se alguém está tentando invadir sua rede?	N	N	N	N	N	N	N	N	N	S	N	**1**	**9%**
9	Você utiliza boas práticas de segurança em relação às senhas de seus dispositivos e rede?	N	N	S	S	N	N	N	N	N	S	N	**3**	**27%**

Observou-se que muitos usuários ao preencher o questionário informavam que as precauções eram aplicadas apenas ao ambiente de seu trabalho, até mesmo por questões obrigatórias. Nesta etapa foram aplicados técnicas de Engenharia Social, e em uma das entrevistas, ao explicar o conceito de boas práticas de segurança em relação às senhas, o proprietário da rede nos forneceu sua senha, porém nesta etapa não foi aplicada qualquer medida corretiva a esse tipo de situação, o alerta foi feito na entrega dos relatórios finais.

O dicionário de senhas utilizado é composto por um conjunto de palavras dos dicionários das línguas portuguesa do Brasil e da língua inglesa dos Estados Unidos (retirado do software *LibreOffice* 4.2.1), apenas com palavras compostas com mais de oito caracteres, além das mil senhas mais utilizadas no mundo de acordo Burnett (2011) e com e palavras de dialetos amazonenses definidas por Marchini (2010). Em complementação, também foi utilizado o dicionário de senhas do sistema operacional *Kali*. Os diversos dicionários acima foram concatenados em apenas um, com o seguinte comando: *$cat wordlist1.txt wordlist2.txt wordlist3.txt >wordlist_final.txt*.

3.3. Coleta e Análise dos Dados das Redes Wireless

Para a localização e associação de cada proprietário das redes *wireless* definidas no escopo, foi utilizado o software *Wi-fi Analyzer*, por meio da medição da intensidade do sinal conforme o deslocamento.

Nos testes de intrusão realizados nas redes com as vulnerabilidades WEP, WPA e WPA2, foram utilizadas as ferramentas *Airmong-ng* para ativar o modo monitoramento na placa de rede *wireless*, o *Airodump-ng* para gerar os arquivos de captura da rede alvo e o *Aircrack-ng* para a decodificação da senha. A Figura 2 exibe o resultado bem-sucedido desse teste de intrusão.

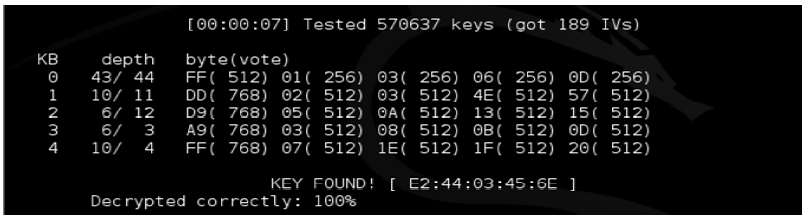


Figura 2. Teste de intrusão com vulnerabilidade WEP

Especificamente para os testes de intrusão com as vulnerabilidades WPA e WPA2, a ferramenta *Aircrack-ng* foi utilizada associada ao dicionário de senhas pré-elaborado. A Figura 3 exibe o resultado bem-sucedido desse teste de intrusão.

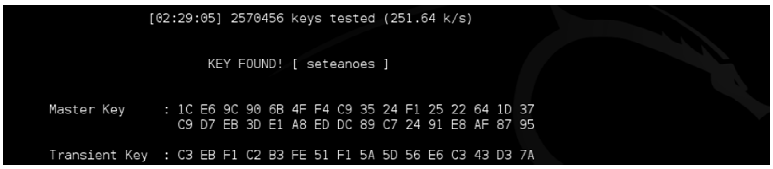


Figura 3. Teste de intrusão com vulnerabilidade WPA com dicionário de senhas

Para a identificação das redes com vulnerabilidade relacionadas ao *WPS*, foi utilizada a ferramenta *Wifite*, conforme mostra a Figura 4.

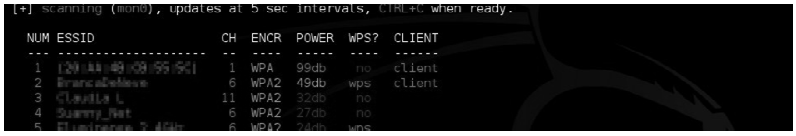


Figura 4. Identificação das redes com *WPS* habilitado

Após a ferramenta *Airmong-ng* ativar o modo monitoramento na placa de rede *wireless*, foi utilizada a ferramenta *Reaver* para a quebra da vulnerabilidade, conforme mostra a Figura 5.

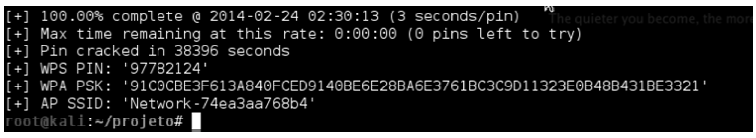


Figura 5. Teste de intrusão em redes com WPS habilitado

Também foi realizado o teste de intrusão chamado “Homem no Meio” (*Man in the Middle*) com *honeypot*. Após compartilhar a conexão, foi ativado o modo de monitoramento da placa de rede *wireless*. Em seguida, foi criado um Ponto de Acesso com o mesmo SSID e no mesmo canal através da ferramenta *Airbase-ng*. Com a associação a essa rede falsa, é possível monitorar o tráfego com a ferramenta *Wireshark*, conforme mostra a Figura 6.

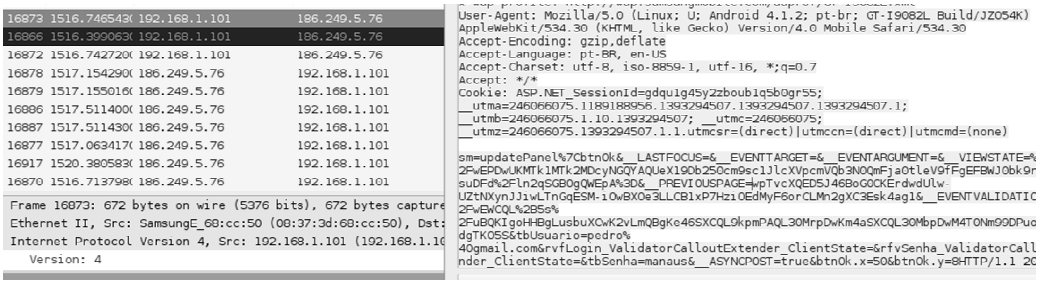


Figura 6. Teste de intrusão do tipo Homem no Meio

4. Resultados Obtidos

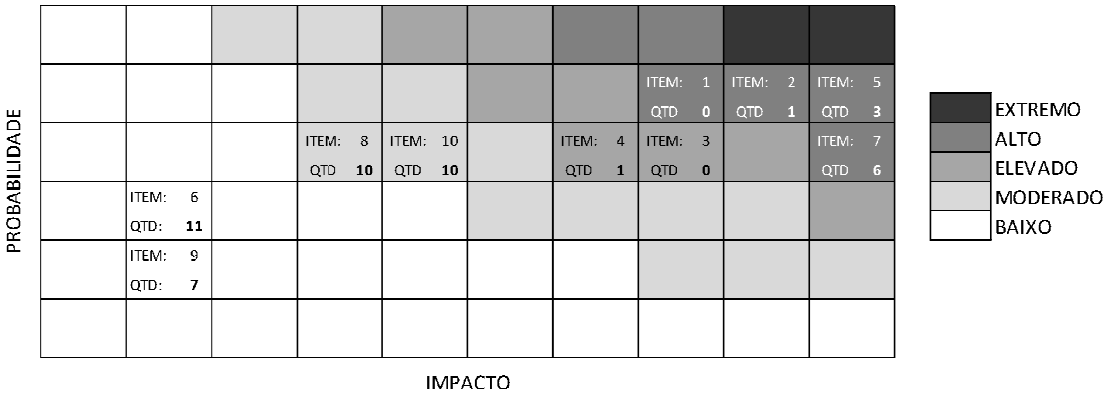
Após as fases mencionadas nas seções anteriores, verificou-se que foram encontradas 49 vulnerabilidades, baseadas nas boas práticas citadas na seção 2.6, como podem ser analisadas na Tabela 2:

Tabela 2. Verificação das vulnerabilidades encontradas

Item	Verificação x – Vulnerabilidade encontrada	WiFi 01	WiFi 02	WiFi 03	WiFi 04	WiFi 05	WiFi 06	WiFi 07	WiFi 08	WiFi 09	WiFi 10	WiFi 11	Total	Percentual
1	Modo de Operação												**0**	**0%**
2	Tipo de Autenticação / Criptografia						x						**1**	**9%**
3	SSID padrão de fábrica												**0**	**0%**
4	Senha de administração de fábrica						x						**1**	**9%**
5	Complexidade de senhas de conexão	x					x		x				**3**	**27%**
6	Difusão do SSID (Broadcast)	x	x	x	x	x	x	x	x	x	x	x	**11**	**100%**
7	Wi-Fi Protected Setup (WPS)	x		x		x	x	x				x	**6**	**55%**
8	Verificação / Manutenção dos equipamentos	x	x	x	x	x	x	x	x	x		x	**10**	**91%**
9	Desligar equipamento quando não usado	x	x	x	x	x		x			x		**7**	**64%**
10	Suscetível à Engenharia Social	x	x	x	x	x	x	x	x	x		x	**10**	**91%**
		Total											**49**	

Para enfatizar e destacar o risco das vulnerabilidades encontradas foi utilizado o cálculo apresentado na fase de Relatório do PTES (risco = probabilidade x impacto), conforme pode ser observado no Quadro 2. Foram detectadas: dez vulnerabilidades consideradas com risco alto, uma com risco elevado, vinte com risco moderado e dezoito com risco baixo.

Quadro 2. Nível de riscos encontrados de acordo com o *PTES*



Diante da análise de risco, foi construído um relatório final para cada proprietário das redes do escopo. O relatório contém informações como: qual seu objetivo, os pontos analisados da rede (verificação, análise e *status*), as conclusões e as sugestões para cada vulnerabilidade encontrada. De acordo com os resultados, foram destacadas ao proprietário as informações de conscientização relacionadas à segurança, adicionalmente foram entregues cartilhas da CERT.br sobre o assunto (em formato impresso e CD), e para as vulnerabilidades encontradas com risco alto e elevado, foram

realizadas as correções presencialmente. Ao entregar os itens mencionados, o proprietário assinava um protocolo de entrega e informava o grau de satisfação quanto à atividade aplicada em sua rede *wireless* doméstica. Dentre as redes analisadas, os proprietários consideraram a avaliação da atividade proveitosa.

5. Conclusão

Observou-se que, em razão da popularização da *internet*, a quantidade de pontos de acesso em ambientes residenciais cresce proporcionalmente, e devido a isso, os fabricantes de pontos de acesso entregam seus produtos com assistentes de configuração simplistas com o intuito de permitir que o próprio usuário final efetue a instalação e configuração do equipamento *wireless*. Entretanto, foi demonstrado que, apesar das facilidades encontradas, as redes *wireless* domésticas estão suscetíveis a vários tipos de ataques, sendo que a maior parte pode ser mitigada através de configurações mais específicas orientadas por meio de profissionais da área de segurança da informação.

Diante disso, a utilização das boas práticas sugeridas pode minimizar, de forma significativa, a incidência de vulnerabilidades nas redes *wireless*, ressaltando que ao preocupar-se com a segurança de sua rede *wireless* o proprietário está protegendo não apenas suas informações, como também as de familiares que residem na mesma residência ou que são utilizadores da mesma rede *wireless*.

Observou-se também que em complemento às boas práticas, é possível aplicar uma metodologia, que mesmo voltada para o ambiente corporativo, se adéqua satisfatoriamente ao ambiente doméstico, quando se trata da análise de vulnerabilidades, desde que suas fases sejam adaptadas de acordo com o cenário escolhido.

Portanto, é possível afirmar que, após a atividade de conscientização com a entrega das cartilhas e sugestões de melhorias às vulnerabilidades encontradas e apresentadas nos relatórios, foi perceptível o aumento da preocupação e interesse por parte dos proprietários quanto às suas redes *wireless* domésticas.

5.1. Trabalhos Futuros

Neste artigo foram identificados alguns pontos de melhoria com o intuito de obter resultados mais aprofundados e, principalmente, empregar em novos cenários. Sendo assim, com base nos resultados descritos anteriormente, ressaltam-se algumas sugestões de trabalhos que podem ser explorados futuramente:

A aplicação de técnicas de *pentest* em cenários como *shopping*s *centers*, aeroportos, restaurantes e demais lugares públicos que fornecem internet gratuita aos seus clientes.

A metodologia PTES possui um direcionamento linear de ações e procedimentos, sendo assim é possível que uma distribuição *Linux* possa ser personalizada para automatizar os métodos de *pentest* e diminuir a carga de conhecimento técnico necessário para realizá-lo, permitindo que usuários leigos avaliem suas próprias redes pessoais domésticas.

6. Referências

BURNETT, Mark. **10.000 Top Passwords**. 2011. Disponível em: https://xato.net/about/#.UxtkgfldXpU. Acessado em: 30 jan. 2014.

Cartilha de Segurança para Internet, versão 4.0 / CERT.br – São Paulo: Comitê Gestor da Internet no Brasil, 2012.

FLICKENGER, Rob et al. **Redes sem fio no Mundo em Desenvolvimento: Um guia prático para o planejamento e a construção de uma infra-estrutura de telecomunicações**, 2008. Projeto E-book. Tradução: Cesar Brod. Disponível em: http://wndw.net. Acessado em: 22 jan. 2014.

HOROVITS, H.; SILVA, E. **Explorando vulnerabilidades em redes sem fio: usando as principais ferramentas de ataque e configurações de defesa.** 2013. Faculdade Senac – DF. Disponível em: http://www.edilms.eti.br/uploads/file/orientacoes/seg02%20Henrique%20Daniel%20Horovits%20-TCC.pdf. Acessado em: 30 jan. 2014

MARCHINI, Silvio. **Amazonário: dicionário das coisas da Amazônia.** 2010. Disponível em: http://www.amazonarium.com.br/blog/?p=281. Acessado em: Acessado em: 30 jan. 2014.

MOREIRA, A.; ARAÚJO, J. e FERREIRA, R. **Avaliação de Segurança em Redes Sem Fio**. 2011. 8th CONTECSI International Conference on Information Systems and Technology Management, USP/São Paulo – SP. Disponível em: http://si.lopesgazzani.com.br/docentes/marcio/ori_g/20110602_JairoRodrigues_AvaliacaoDeSegurancaEmRedesSemFio.pdf . Acessado em: 24 jan. 2014.

PINZON, Alexandre. **Vulnerabilidade da Segurança em Redes Sem Fio**. Centro Universitário Ritter dos Reis – UniRitter. Porto Alegre, 2009. Disponível em: http://www.uniritter.edu.br/graduacao/informatica/sistemas/downloads/tcc2k9/TCCII_2009_1_Alexandre.pdf . Acessado em: 23 jan. 2014.

*PTES. **Tecnhical Guidelines***, 2012. Disponível em: http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines. Acessado em: 10 jan. 2014.

RAMACHANDRAN, Vivek. **BackTrack 5 Wireless Penetration Testing**. 2011. Packt Publishing Ltd.

RUFINO, Nélson M. De O. **Segurança em redes sem fio: aprenda a proteger suas informações em ambientes Wi-fi e Bluetooth**. 3 ed. São Paulo: Nova Editora, 2011.

SERIQUE JUNIOR, L.; SILVA, C. e SILVA, E. **Boas práticas de segurança para redes domésticas: Instalação e configuração de ativos para torná-las seguras**. 2012. Faculdade Senac – DF. Disponível em: http://www.edilms.eti.br/uploads/file/orientacoes/seg02%20Clecyone%20Carlo20d%2 0Silva.pdf . Acessado em: 15 jan. 2014.

TIC Domicílios e Empresas 2012: **Pesquisa sobre o Uso das Tecnologias de Informação e Comunicação no Brasil**. Comitê Gestor da Internet no Brasil – CGI.br. São Paulo: 2013. Disponível em: http://www.cetic.br/publicacoes/2012/tic-domicilios-2012.pdf. Acessado em: 22 jan. 2014.

WILHELM, Thomas. **Professional Penetration Testing Creating and Operating a Formal Hacking Lab**. Rockland, Massachusetts: Syngress. 2010.