Segurança na Internet das Coisas: Varredura, Análise e Estatística de Redes sem Fio em Bom Jesus do Itabapoana

Ana Julia B. Alves[1], Wesley Folly V. de Souza[2]

[1]Instituto Federal Fluminense – Bom Jesus do Itabapoana – RJ – Brasil

[2]Coordenação de Informática – Instituto Federal Fluminense – Bom Jesus do Itabapoana – RJ – Brasil

{anajuliabritesalves,wesleyfolly}@gmail.com

Abstract. In this work we will do a research with the aid of the wardriving method so that we can find out how much Wi-Fi networks in our region are vulnerable to attacks. To this end, we will capture and analyze data such as: security protocols, wps configurations, radio channels, device discrimination, among others.

Resumo. Neste trabalho foi realizada uma pesquisa com o auxílio do método *wardriving* para que possamos descobrir o quanto as redes *Wi-fi* da região estão vulneráveis a ataques. Com esse objetivo, foi realizada a captura e análise de dados como: protocolos de segurança, configurações wps, canais de rádio, discriminação de dispositivos, entre outros.

1. Introdução

As redes sem fio apresentam um problema em relação às redes cabeadas: as vulnerabilidades e riscos são maiores, pois suas ondas eletromagnéticas atravessam o ar, paredes e muitos obstáculos tornando-se (caso a segurança da rede não seja muito bem planejada) um alvo perfeito para captura de informações de acordo com Oliveira (2010).

Diversos ataques podem ser feitos contra redes e dispositivos sem fio, especialmente se o atacante tiver acesso a informações como status da configuração WPS (*Wi-Fi Protected Setup*) do ponto de acesso, redes preferenciais de dispositivos IoT (*Internet of Things*) e protocolos de segurança e criptografia da rede, como WPA*(Wireless Protected Access)*, WEP*(Wired Equivalent Privacy)* e WPA2 (*Wireless Protected Access II*).

Com o advento e popularização de dispositivos IoT, a rede *Wireless* se torna um ponto crítico na segurança destes dispositivos pois a maioria utiliza apenas essa forma de transmissão de dados. Por se conectarem principalmente a redes locais, a segurança implementada nesses dispositivos é fraca. Portanto, o comprometimento das redes sem fio deixa todos os dispositivos conectados a elas vulneráveis segundo Zabadal e Castro (2017).

2. Método

Os equipamentos utilizados foram: um automóvel (figura 1), uma antena externa acoplada a ele (figura 1), um telefone celular da marca LG com Sistema Operacional *Android*, um notebook Lenovo com dual boot dos Sistemas Operacionais *Windows* 10 e o *Ubuntu* 17.10. Foi utilizado o software *Aircrack-NG* [aircrack-ng.org] no sistema *Ubuntu* (figura 2) e o aplicativo *WiGLE-Wifi* [*wigle.net*] no aparelho celular.

Figura 1. Antena e veículo utilizado na varredura.

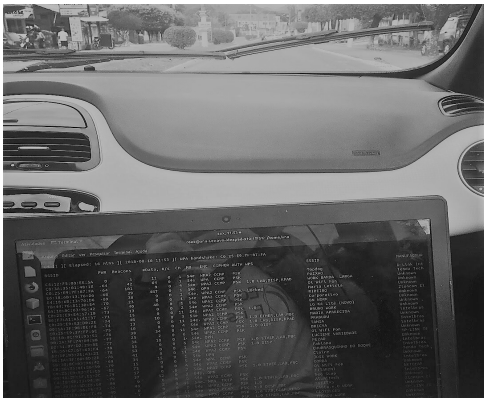

Figura 2. Software utilizado na varredura.

A varredura ocorreu no dia 10/08/2018, a mesma se iniciou no Instituto Federal Fluminense de Bom Jesus do Itabapoana e terminou nesse mesmo ponto, visto que foi feito um trajeto de retorno, totalizando um deslocamento de aproximadamente 5 Km.

A figura 3 mostra a distribuição desses pontos de acesso sobrepostos ao mapa da cidade de Bom Jesus do Itabapoana disponibilizado pelo *Google Earth [Google]*.

Figura 3. Distribuição de pontos de acesso na zona comercial da cidade de Bom Jesus do Itabapoana.

3. Análise dos resultados

O *Aicrack-NG* conseguiu capturar dados de aproximadamente 850 redes *Wireless* durante a varredura. Os dados escolhidos para estatística e análise foram: protocolos de

segurança, status do WPS e visibilidade de redes preferenciais nos dispositivos.

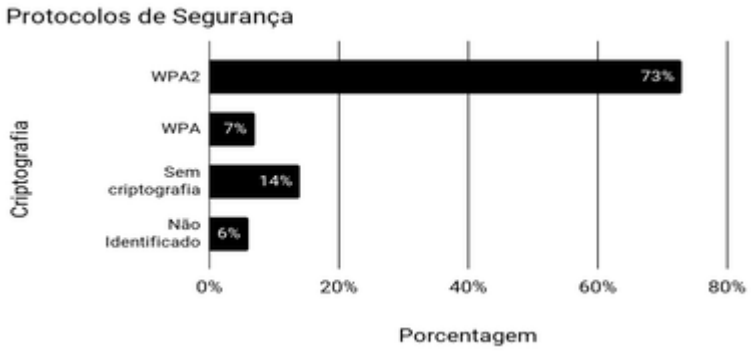

Figura 4. Protocolos de Segurança.

A figura 4 mostra que 73% das redes sem fio locais estão protegidas, pois usam o protocolo WPA2, porém 7% possui o protocolo WPA, que não é tão seguro como dito por Lashkari, Danesh e Samadi (2009) e 14% das redes não usam criptografia alguma, ou seja, os dados dos usuários da rede ficam totalmente expostos a invasores.

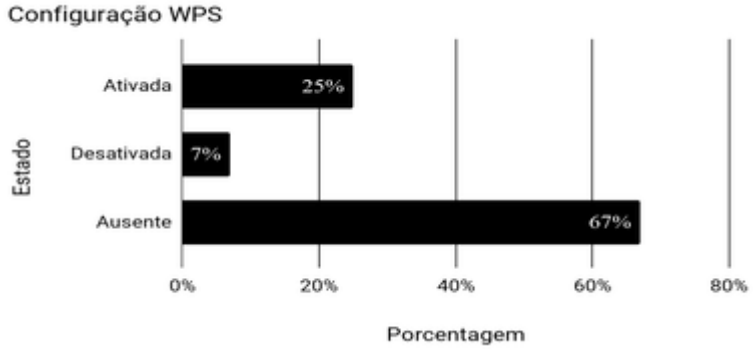

Figura 5. Ocorrência de ativação da configuração WPS.

Segundo a figura 5, a WPS não foi encontrada em muitas redes, o que significa que roteadores atuais estão deixando de ter essa opção habilitada por padrão, ou até mesmo que não usem mais ela. Mas, 25% estão com a WPS ativada, deixando a rede vulnerável mesmo que esta utilize o WPA2 e uma senha forte segundo Silva (2014).

Figura 6. Status da visibilidade das redes preferenciais nos dispositivos.

Conforme a figura 6, é possível notar que a maioria dos dispositivos ocultam suas redes preferenciais, o que é um ótimo indicativo de segurança. Mas, o número de usuários conectados às redes sem fio que foram rastreados pela ferramenta foi menor devido ao deslocamento do automóvel, portanto não se pode afirmar que essa índice é confiável.

Vale ressaltar que apenas redes fixas foram analisadas, não incluindo, portanto, redes 3G e 4G.

4. Conclusão

Dado o exposto pode-se perceber que os dados relacionados à segurança dos dispositivos e redes da cidade são promissores, acredita-se que isso se deve ao fato de ser uma zona predominantemente comercial e portanto os usuários terem uma preocupação maior com a segurança e dessa forma terem posse de equipamentos modernos e configurados cuidadosamente por mão de obra especializada, porém ainda há vulnerabilidades que devem ser corrigidas para evitar furto de dados não autorizados.

Referências

OLIVEIRA, A. T. (2010) “Análise das Vulnerabilidades das Redes Sem Fio na Cidade de Vitória da Conquista-BA”,73 f. TCC (Graduação) - Curso de Ciência da Computação, Ciências Exatas, Universidade Estadual do Sudoeste da Bahia, Vitória da Conquista – Ba , http://www2.uesb.br/computacao/wp-content/uploads/2014/09/ANÁLISE-DAS-VULNERABILIDADES-DAS-REDES-SEM-FIO-NA-CIDADE-DE-VITÓRIA-DA-CONQUISTA-BA-Alan-Teixeira-de-oliveira.pdf.

Arash Habibi Lashkari, Mir Mohammad Seyed Danesh and B. Samadi (2009) , "A survey on wireless security protocols (WEP, WPA and WPA2/802.11i)," 2nd IEEE International Conference on Computer Science and Information Technology, Beijing, pp. 48-52.

SILVA, Cristiano de Souza (2014). VULNERABILIDADE DO WPS (WI-FI PROTECTED SETUP) NAS REDES SEM FIO. 20 f. Artigo - Curso de Perícia Digital, Universidade Católica de Brasília, Brasília. Disponível em: https://sistemas.stf.jus.br/dspace/xmlui/bitstream/handle/123456789/1189/Monografia%20-%20Cristiano%20de%20Souza%20e%20Silva.pdf?sequence=1&isAllowed=y. Acesso em: 01 mar. 2020.

ZABADAL, Bernardo Moreira; CASTRO, Bianca Francinny Lisboa Murta de (2017). IoT e Seus Principais Desafios. 10 f. Artigo. Instituto Federal de Educação, Ciência e Tecnologia de São Paulo, São Paulo.Disponível em: http://rinte.ifsp.edu.br/index.php/RInTE/article/view/333/pdf_94. Acesso em: 01 mar. 2020.