ANÁLISE DE VULNERABILIDADES EM REDES SEM FIO: UMA FERRAMENTA PARA DIAGNÓSTICO E SUGESTÃO DE CONTRAMEDIDAS PARA ROTEADORES

WESLEN S. DE SOUZA[1]; MARILTON S. DE AGUIAR[1]

[1]Universidade Federal de Pelotas – {wsdsouza,marilton}@inf.ufpel.edu.br

1. INTRODUÇÃO

As redes de internet sem fio têm ganhado muita popularidade em diversas áreas, onde comumente são utilizadas entre usuários domésticos de microcomputadores para criar pontos de acesso à internet. A primeira criptografia amplamente empregada foi a WEP (*Wired Equivalent Privacy*) que apresentava a proposta de ter a mesma segurança das redes cabeadas, porém mais tarde provou-se que esta apresentava diversas falhas, mas continuou sendo usada por muitos anos, já que a quantidade de computadores não era expressiva e não haviam preocupações com a privacidade ou com a segurança das informações que trafegavam (ZAJMOVIC, 2015).

As redes Wi-Fi, apesar de estarem bastante difundidas e terem constante aumento no número de usuários, ainda são muito inseguras por diversos fatores, tais como: a utilização de técnicas de criptografias obsoletas, modelos de roteadores inseguros e defasados, roteadores mal configurados ou desatualizados. Os usuários domésticos com pouco conhecimento na área de segurança da informação são os mais afetados por problemas de segurança, pois não sabem definir se a rede que acessam tem uma conexão segura. Utilizar uma rede desprotegida pode ocasionar na quebra da confiabilidade, integridade e autenticidade dos dados do usuário.

Muitas vezes os usuários estão utilizando redes Wi-Fi despercebidamente, o que é muito comum na utilização de *smartphones*, seja através de dados móveis ou através de redes Wi-Fi. Normalmente os *smartphones* tem como padrão fazer a conexão de forma automática em redes Wi-Fi que o usuário já tenha utilizado, mesmo que este já esteja usando os dados móveis do celular, de modo que o aparelho costuma fazer a troca para o Wi-Fi automaticamente, deixando de certa forma implícita qual conexão está sendo usada para acessar a internet, podendo assim comprometer a integridade dos dados do usuário caso a rede apresente algum tipo de vulnerabilidade (LEAVITT, 2011).

Existem ferramentas capazes de detectar tentativas de invasões tais como os WIDS (*Wireless Intrusion Detection System*), porém, essas em sua grande maioria são pagas e todas voltadas apenas para usuários avançados como gerentes de redes, dificultando a utilização por um usuário inexperiente (BOOB; JADHAV, 2010).

Tendo em vista os problemas citados, este trabalho propõe o desenvolvimento de uma ferramenta de segurança para redes Wi-Fi aplicada sobre os principais protocolos usados atualmente, os quais são WEP, WPA e WPA2 que atuará detectando possíveis vulnerabilidades referentes ao protocolo usado na rede em questão. Esta ferramenta será voltada para usuários domésticos onde, a partir de poucas interações, poderão se ter informações sobre a segurança da rede que está sendo utilizada. Caso for detectado algum problema de segurança, a ferramenta irá apresentar uma sugestão de como

corrigi-lo, prevenindo ataques às informações sigilosas de indivíduos por terceiros, contribuindo assim para uma melhor segurança aos usuários.

2. METODOLOGIA

Para o desenvolvimento desta ferramenta entende-se que há a necessidade de um profundo conhecimento do funcionamento dos protocolos WEP, WPA e WPA2 os quais são mais utilizados atualmente em redes Wi-Fi, e também em suas principais vulnerabilidades (FERREIRA, 2014).

Para isto, foram realizados estudos sobre o funcionamento dos protocolos citados, suas principais vulnerabilidades e formas de como sanar estes problemas visando adquirir uma sólida base de conhecimento sobre estes temas para que deste modo a ferramenta seja desenvolvida com todas as funcionalidades previstas e com a maior qualidade possível.

Após o levantamento das principais contramedidas disponíveis para as vulnerabilidades estudadas, foi feita uma análise com o objetivo de identificar a melhor e mais intuitiva forma de apresentar esta contramedida para o usuário final, tendo em mente ainda que este terá pouquíssimo ou nenhum conhecimento da área de segurança da informação.

Foi realizada uma pesquisa para identificar os principais *frameworks* disponíveis na comunidade, que poderiam ser utilizados neste trabalho, visando acelerar o desenvolvimento do mesmo (HOROVITS; SILVA, 2013).

Neste estágio de desenvolvimento, está sendo realizado um estudo para definir sob qual sistema operacional a ferramenta será desenvolvida, tendo como intuito inicial o desenvolvimento desta para a plataforma de dispositivos moveis Android, porém deverá ser levado em consideração a disponibilidade dos *frameworks* e o suporte de *hardware* por parte dos dispositivos móveis.

Posteriormente, deverá ser executado um estudo com casos de testes onde se objetiva verificar o quão efetiva será a ferramenta para a proteção dos usuários e ainda o quão eficiente esta será em relação a identificação de vulnerabilidades (REDDY; LAKSHMI, 2014).

3. RESULTADOS E DISCUSSÃO

No que tange o estudo abrangendo os protocolos WEP, WPA e WPA2, foi realizada uma análise das vulnerabilidades presentes nos mesmos e suas contramedidas de forma. De forma resumida, pode-se citar, em cada protocolo, as seguintes principais vulnerabilidades.

O protocolo WEP apresenta sérias vulnerabilidades de segurança independentemente da configuração adotada pelo ponto de acesso (do inglês, *Access Point* – AP) esse sempre estará sujeito a algum tipo de ataque que poderão comprometer a segurança dos clientes, sendo a principal contramedida para este problema a troca deste protocolo no AP por um que use uma criptografia mais forte (FIGUEIREDO, 2015).

Além disso, foi estudada a vulnerabilidade no algoritmo TKIP, empregado normalmente no protocolo WPA, mas que também pode ser usado pelo protocolo WPA2. Este algoritmo apresenta uma vulnerabilidade onde um usuário mal-intencionado pode capturar os pacotes que trafegam e de criptografar este através de um ataque conhecido como ChopChop, tendo assim acesso às informações sigilosas dos clientes conectados ao AP (HALVORSEN et al.,2009). A principal contramedida para esta vulnerabilidade é a troca nas configurações do

AP do protocolo TKIP para o CCMP que apresenta uma criptografia mais forte e segura.

O método de configuração protegida do Wi-Fi (do inglês, *Wi-Fi Protected Setup* – WPS) foi projetado pela Wi-Fi Alliance para facilitar a configuração de redes domésticas, possibilitando o uso de um código de 8 dígitos para fazer a conexão no AP ao invés da senha secreta da rede sendo este código chamado de PIN. Esse protocolo introduziu uma vulnerabilidade devido a forma na qual foi implementado pelas indústrias. Na Figura 1, apresentada abaixo, pode ser observado que o código em si compreende todo o PIN, mas sim é dividio em três partes, de modo que se o atacante acerta apenas a primeira destas partes, o AP responde avisando que a mesma estaria correta. Desta forma, introduz-se a vulnerabilidade, que possibilita a execução de um ataque por força bruta (MORAIS, 2013). No WPS a principal contramedida é a desativação deste protocolo.

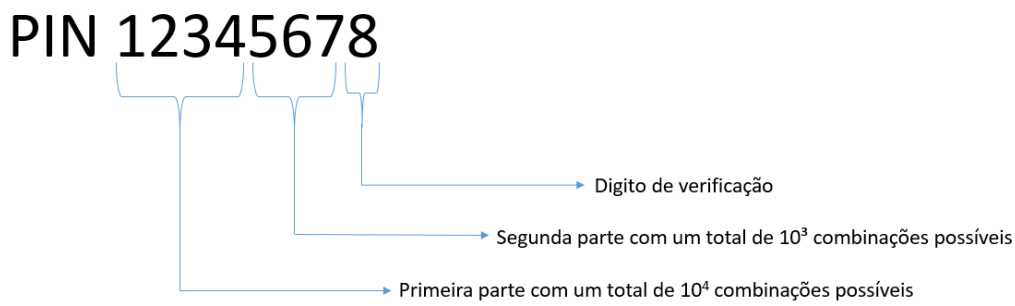

Figura 1 – Esquema gráfico da divisão do código PIN

A ferramenta foi desenvolvida para as plataformas Windows e Linux devido a incompatibilidade do hardware presente nos dispositivos moveis com técnicas de monitoramento de pacotes e ainda a pouca disponibilidade de *frameworks* disponíveis nas mesmas.

Neste momento, a interface gráfica básica da ferramenta e a funcionalidade de detecção de vulnerabilidades foram desenvolvidas, como pode ser verificado na Figura 2. Nesta Figura, exibe-se uma ocasião hipotética, onde um usuário tenta se conectar em uma rede WI-FI vulnerável se deparando com uma tela de aviso e um link para um documento que conterá uma explicação de forma simples e intuitiva de como este poderá sanar este problema.

Figura 2 – Interface da ferramenta

4. CONCLUSÕES

Através desta ferramenta usuários com pouco conhecimento da área de segurança da informação poderão se beneficiar do uso da mesma obtendo informações de forma simples e intuitiva do quão seguras são as redes WI-FI que pretendem acessar e ou estiverem acostumados a usarem em seu cotidiano, proporcionando desta forma uma melhora significativa da segurança das informações destes usuários.

Na continuidade do trabalho, será realizado um estudo com casos de testes onde se objetiva verificar o quão efetiva será a ferramenta para a proteção dos usuários e ainda o quão eficiente esta será em relação a identificação de vulnerabilidades.

5. REFERÊNCIAS BIBLIOGRÁFICAS

BOOB, S.; JADHAV, P. Wireless intrusion detection system. **International Journal of Computer Applications**, [S.l.], v.5, n.8, p.9–13, 2010.

FERREIRA, J. L. M. Segurança em redes sem fio. , [S.l.], 2014.

FIGUEIREDO, D. A. ANÁLISE DA SEGURANÇA DE REDES WI-FI ATRAVÉS DE TESTE DE PENETRAÇÃO EM INSTITUIÇÕES DE ENSINO SUPERIOR DE BELO HORIZONTE. **Projetos e Dissertações em Sistemas de Informação e Gestão do Conhecimento**, [S.l.], v.4, n.1, 2015.

HALVORSEN, F. M.; HAUGEN, O.; EIAN, M.; MJØLSNES, S. F. **An improved attack on TKIP**. In: NORDIC CONFERENCE ON SECURE IT SYSTEMS, 2009. **Proceedings. . .** [S.l.: s.n.], 2009. p.120–132.

HOROVITS, H. D.; SILVA, E. M. Explorando vulnerabilidades em Redes sem Fio: Usando as principais ferramentas de ataque e configurações de defesa. , [S.l.], 2013.

MORAIS, E. M. de. Segurança e ataques em redes Wifi. , [S.l.], 2013.

LEAVITT, N. Mobile security: finally a serious problem? **Computer**, [S.l.], v.44, n.6, p.11–14, 2011.

REDDY, B. S. K.; LAKSHMI, B. Enhanced Security Technique in WPA & WEP Based Wireless (Wi-Fi) Networks. , [S.l.], 2014.

ZAJMOVIC, M.; SABANOVIC, A.; SABIC, S.; PIVIC, D. WIRELESS WI-FI COMPUTER NETWORK AND SECURITY WI-FI NETWORK. **INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES**, [S.l.], p.35, 2015.