Desenvolvimento de uma Metodologia para Auditoria em Redes Sem Fio IEEE 802.11b/g

Fabiano Silva, Glauco Antonio Ludwig

Universidade do Vale do Rio dos Sinos (UNISINOS)
Caixa Postal 750 – 93.022-000 – São Leopoldo – RS – Brasil
fabiano.silva@brturbo.com.br, glaucol@unisinos.br

Abstract. *Wireless network deployment is growing quickly nowadays. Mobility, convenience and easy setup are some of advantages on using it, however, innumerous security threats need to be concern. The main goal of this research it to develop a methodology to proceed wireless network audit under IEEE 802.11. As expected result, it intend to help professionals persons of infrastructure and security network areas with the hardest mission of keep wireless environment available and safe.*

Resumo. *A implementação de redes sem fio vem crescendo rapidamente nos dias de hoje. A mobilidade, a conveniência e a facilidade de instalação e configuração são algumas das vantagens no uso dessas redes, entretanto, existem inúmeras brechas de segurança que precisam ser consideradas. Visando identificar e tratar essas vulnerabilidades, a presente pesquisa tem como objetivo a elaboração de uma metodologia para auditar as redes sem fio IEEE 802.11. Como resultado, espera-se que essa iniciativa possa auxiliar profissionais das áreas de infra-estrutura e segurança de redes na difícil tarefa de manter o ambiente sem fio disponível e seguro.*

1. Introdução

A tecnologia de redes sem fio, em inglês chamada de *Wireless Networks* (WLAN) ou apenas *Wi-Fi*, é hoje uma das mais populares e com maior crescimento de mercado. Segundo a Dell'Oro Group, empresa focada na pesquisa e análise de mercado na área de telecomunicações, o uso de redes sem fio vem crescendo cerca de 34% ano após ano [INCISOR 2007]. A produção de equipamentos sem fio em larga escala a preços acessíveis aos consumidores, somado a facilidade de instalação e configuração, são fatores que contribuem para esse crescimento. A Cisco, empresa fabricante de equipamentos de redes e que possui cerca de 66% do mercado sem fio, anunciou em abril do ano passado um marco em sua história: a produção de mais de quatro milhões de *Access Point*[1] (AP) [CISCO 2007].

1.1. Motivação

As vantagens no uso dessa tecnologia são inúmeras. A mobilidade é sem dúvida a maior delas, possibilitando o acesso a informação em qualquer lugar a qualquer hora [Karmakar e Dooley 2008]. O aumento da produtividade é outro ponto importante no uso de redes sem fio, independente da área, seja ela indústria, serviço, saúde, governo, etc. Em um escritório que faz uso desse tipo de tecnologia, o empregado não fica limitado apenas a sua mesa de

[1] *Access Point* é o equipamento que realiza a interconexão entre os dispositivos móveis em uma rede *wireless*.

trabalho: é possível ir a uma sala de reuniões ou a um outro lugar qualquer da empresa sem perder a conectividade com a rede.

No entanto, o que muitas pessoas ignoram, ou simplesmente não julgam ser importante, é o fato desses benefícios ocultarem graves problemas relacionados à segurança das informações. Em uma rede sem fio, a informação é enviada em todas as direções em forma de ondas eletromagnéticas [Miyoshi e Sanches 2002]. Assim, uma pessoa mal intencionada e com o correto equipamento pode facilmente capturar essas informações e usá-las de forma indevida.

Atualmente, na tentativa de resolver ou minimizar esse problema, existem alguns mecanismos de segurança que podem ser adotados, como a criptografia. No entanto, foi provado que esses mecanismos não são completamente adequados para a comunicação segura em redes sem fio [Karmakar e Dooley 2008]. Sabe-se também que não é possível ter uma rede totalmente segura, no entanto, é possível controlar os riscos através do monitoramento e da realização de auditorias periódicas. Essas duas práticas somadas aos mecanismos de segurança podem minimizar os riscos de incidentes como a perda ou o roubo de informações.

Auditar redes sem fio de maneira sistêmica e efetiva é um grande desafio. A análise dos dados coletados durante uma auditoria, em tempo hábil à identificar problemas de segurança, é a maior dificuldade enfrentada por analistas de infra-estrutura. Empresas de auditoria em sistemas oferecem esse serviço, entretanto, não existe hoje uma metodologia formalizada para tal. Baseado nessa premissa que a presente pesquisa se fez necessária.

1.2. Objetivos

O objetivo geral desse trabalho é propor uma metodologia para auditoria em redes sem fio IEEE 802.11b/g com foco na segurança da informação.

Para atingir essa finalidade, alguns objetivos específicos foram definidos:

1. Pesquisar os principais problemas atualmente relacionados à segurança da informação em redes sem fio;

2. Pesquisar as alternativas para solucionar esses problemas bem como as ferramentas e técnicas empregadas;

3. Estudar um caso de rede sem fio onde exista uma política ou sistemática de auditoria, fazendo uma análise sob o ponto de vista dos problemas identificados no primeiro objetivo específico;

4. Propor melhorias para o estudo de caso em questão;

5. Estruturar uma metodologia genérica para auditoria.

1.3. Contribuições

Com a conclusão dessa pesquisa, prevista para o final de 2008, espera-se que a metodologia proposta possa auxiliar analistas de infra-estrutura e segurança de rede na árdua tarefa de manter o ambiente *wireless* disponível e seguro.

1.4. Organização do Texto

O presente texto está organizado da seguinte forma: na seção dois são abordados alguns conceitos básicos do processo de auditoria; a seção três apresenta algumas das vulnerabilidades relacionadas com o uso da tecnologia sem fio; já na seção quatro, é

demonstrado uma versão parcial da estrutura da metodologia proposta, bem como uma breve explicação dos seus passos; e por fim, algumas conclusões e projeções para as próximas atividades dessa pesquisa são apresentadas na seção cinco.

2. O Processo de Auditoria

Sob o ponto de vista da tecnologia da informação, todos os processos e sistemas em uma organização existem para atender às necessidades do negócio. O correto funcionamento desses processos são fatores fundamentais para que a organização atinja os seus objetivos. Isso é o que justifica a criação dos controles internos.

Avaliar o estado atual desses controles é o que objetiva uma auditoria. Segundo [Davis, Schiller e Wheeler 2007], os controles internos são os mecanismos que garantem o funcionamento correto dos processos. O papel do auditor é identificar a existência de riscos ou ameaças aos processos, e assegurar que os controles são adequados às necessidades do negócio. Ainda segundo os mesmos autores, esses controles podem ser classificados em três tipos: de prevenção, de detecção e de reação. Já suas implementações podem ser: administrativas, técnicas e físicas.

Controles de prevenção são aqueles que evitam que algo aconteça. Por exemplo, solicitar a identificação de usuário e senha para acessar uma aplicação previne, teoricamente, que pessoas não autorizadas acessem o sistema. Já os controles de detecção são aqueles que permitem identificar que algo ocorreu. Um arquivo de *log* com todas as transações efetuadas no sistema é um exemplo. Por fim, controles de reação, ou corretivos, não impedem que algo aconteça, no entanto, permitem uma sistemática para identificar que algo aconteceu e corrigir a situação. Um exemplo de controles corretivos são as ferramentas de monitoração de rede como o *NNM* [Hewlett-Packard 2008]. Essa ferramenta representa graficamente a topologia da rede e utiliza um esquema de cores (verde: ativo; amarelo: parcialmente ativo; vermelho: inativo) para identificar o status de cada equipamento.

Já com relação às implementações, as administrativas são as políticas que regem o funcionamento de um sistema. Permitir somente senhas seguras, com oito ou mais dígitos e contendo números, letras maiúsculas e minúsculas, é um exemplo. Já as implementações técnicas são as ferramentas de software ou hardware que asseguram essas políticas. O *Microsoft Active Directory* (AD) pode ser citado como um exemplo de software que implementa, tecnicamente, a política de senhas do exemplo anterior. Por fim, as implementações físicas, como o próprio nome diz, são aquelas que garantem a integridade física de algo. Por exemplo, o controle de acesso restrito por portas de segurança à sala dos servidores.

De acordo com [Davis, Schiller e Wheeler 2007], uma auditoria pode ser dividida em seis grandes fases, como mostra a Figura 1.

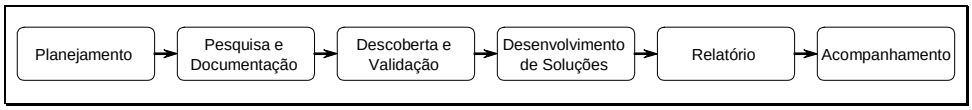

Figura 1. As seis fases de uma auditoria [Davis, Schiller e Wheeler 2007].

- Planejamento: nessa etapa são definidos os objetivos e o escopo da auditoria. É elaborada uma lista com os passos a serem seguidos. O mau planejamento compromete o resultado da auditoria;

- Pesquisa e documentação: é a etapa mais longa da auditoria. Nessa fase são seguidos os passos definidos anteriormente. Durante a pesquisa, o auditor coleta e analisa dados dos processos. O resultado final é um documento contendo todos os pontos observados e os riscos em potencial associados;
- Descoberta e validação: nessa etapa o auditor deve validar com o responsável da área auditada todos os riscos apontados na pesquisa. Devem ser considerados os riscos que realmente representam ameaças ao negócio em questão;
- Desenvolvimento de soluções: uma vez identificados e validados os problemas, é necessário desenvolver um plano de ação. Geralmente o auditor propõe algumas soluções, cabendo ao responsável da área a escolha da mais adequada. No plano de ação devem constar os nomes dos responsáveis pela execução do plano bem como uma data prevista para conclusão;
- Relatório: nessa etapa o auditor gera o relatório final com os resultados da auditoria. A estrutura deste documento pode ter várias formas, no entanto, três itens são essenciais: a) Escopo, deixando claro o que estava incluso na auditoria e, caso necessário, o que não estava; b) Sumário, constando uma visão geral do resultado da auditoria e, de forma resumida, os principais problemas encontrados e as ações a serem adotadas; e c) Lista dos problemas e planos de ação, apresentando de forma detalhada os problemas apontados durante a auditoria e os planos para resolvê-los;
- Acompanhamento: o processo de auditoria não termina com a entrega do relatório, é preciso garantir que todos os problemas foram resolvidos. Nessa etapa, portanto, o auditor deve agendar reuniões periódicas com os responsáveis pelos planos de ação.

3. Vulnerabilidades e Ameaças

Em virtude do meio físico utilizado, a Radio Freqüência (RF), as redes *wireless* possuem uma vulnerabilidade intrínseca em sua aplicação [Karmakar e Dooley 2008]. As ondas de rádio se propagam no espaço, transpassando paredes e outros obstáculos, permitindo facilmente que pessoas não autorizadas as interceptem [Khadraoui e Herrmann 2007]. A área de cobertura das WLANs, segundo os padrões do IEEE 802.11b/g, varia em função de alguns fatores, tais como: potência de saída, tipo de antena, tipo do ambiente, entre outros. Comercialmente, os *Access Point* equipados com antenas do tipo *omni-direcionais*[2], possibilitam um raio de cobertura de 35 a 40 metros em ambientes fechados, e de 120 a 140 metros em ambientes abertos. No entanto, com o uso de antenas direcionais, é possível capturar o sinal de um AP a mais de um quilômetro de distância [Karmakar e Dooley 2008]. Abaixo estão listadas algumas das principais ameaças às redes *wireless*.

3.1. Negação de Serviço (*Denial of Service* - DoS)

Semelhante às redes estruturadas, o objetivo de um ataque DoS é tornar a rede indisponível [Khadraoui e Herrmann 2007]. Esse tipo de ameaça é facilmente identificada, porém, muito difícil de evitar. Os principais tipos de ataques DoS em WLANs são:

a) Bloqueio de Onda (*Jamming the Air Waves*): ocorre quando duas antenas próximas utilizam o mesmo canal para transmissão no mesmo instante de tempo. O uso de

[2] *Omni-direcionais* ou dipolo, são antenas que irradiam energia igualmente em todas as direções do seu eixo.

equipamentos que compartilham a mesma faixa de freqüência, como telefones sem fio e dispositivos *Bluetooth*, geram interferência nas redes *Wi-Fi* provocando esse problema;

b) Sobrecarga de Acesso (*Rush Access*): consiste em enviar um número excessivo de requisições de acesso a um mesmo *Access Point*, gerando uma sobrecarga e, conseqüentemente, tornando-o indisponível;

c) Falsificação dos Frames de des-autenticação (*Spoofed de-autentication frames*): o propósito desse ataque é falsificar a requisição de des-autenticação, normalmente enviada por uma estação ao AP durante o processo de desconexão. Nesse caso, o atacante consegue facilmente desconectar todos os clientes da rede.

3.2. *Man-in-the-Middle* (MITM)

Neste tipo de ataque, o cliente *wireless* (vítima) tem sua conexão desviada para um falso *Access Point*, implementado pelo atacante [Hurley 2007]. Esse por sua vez encaminha a conexão para o AP originalmente de destino. Esse tipo de ataque também é conhecido como *Fake AP* [Khadraoui e Herrmann 2007], e tem como objetivo manipular os dados do cliente sem que esse perceba que a conexão foi comprometida.

3.3. *Rogue AP*

Consiste em conectar um *Access Point* ilegal a rede estruturada. Isso permite que um atacante, por exemplo, tenha fácil acesso a todos os serviços da rede [Khadraoui e Herrmann 2007]. Muitas vezes esse tipo de ataque é inocentemente provocado por um usuário que, no intuito de melhorar o seu ambiente de trabalho, conecta à rede o seu AP particular. Essa vulnerabilidade é muito comum em redes de grande porte, e potencialmente perigosa, pois além de alterar a topologia compromete a segurança da informação.

3.4. *Scanning*

Este ataque tem como objetivo identificar os *Access Points* e capturar o tráfego da rede. Existem duas maneiras para identificar uma WLAN, através do modo passivo ou do modo agressivo [Mcclure, Scambray e Kurtz 2005]. A primeira consiste em capturar os pacotes de *beacons*[3], enviados periodicamente pelo AP. Não há como identificar esse tipo de *scanning*, visto que não gera dados na rede. Já na segunda, o atacante envia os pacotes *beacons* de pesquisa, forçando o *Access Point* a enviar uma resposta com os seus dados. Uma vez identificada a rede, é possível iniciar a captura dos dados. Para isso, se faz necessário o uso de ferramentas de software do tipo *Wireless Sniffers*, como o *Kismet* [Kershaw 2008], por exemplo [Mcclure, Scambray e Kurtz 2005].

3.5. *Wardriving*

Esta é uma técnica que utiliza o mesmo princípio do *Scanning* e consiste em dirigir ao redor de uma área específica, mapeando a população de Access Points com um propósito estatístico [Hurley 2007]. O termo *Wardriving* muitas vezes é substituído por *Wireless Footprinting*, pois essa não requer necessariamente que seja feita com o auxílio de um automóvel, é possível implementá-la caminhando ao redor da área em estudo [Mcclure, Scambray e Kurtz 2005]. Os dados coletados podem ser analisados de várias formas, por exemplo, para gerar alertas de segurança ou até mesmo para identificar conflitos de canais. No entanto, essa técnica pode ser empregada para planejar ataques às WLANs.

---

[3] *Beacons* são *frames* curtos usados nas conexões *wireless* para sincronizar a comunicação.

3.6. *Warchalking*

Semelhante ao *Wardriving*, porém com o objetivo de marcar as áreas onde é possível acessar a Internet através das redes *Wi-Fi* [Khadraoui e Herrmann 2007]. Criada por Matt Jones em junho de 2002, esse ataque padroniza o uso de símbolos, como mostra a Figura 2. Esses símbolos, geralmente desenhados em paredes ou no chão, contém informações importantes sobre a rede, tais como: *Service Set Identity*[4] (SSID), largura de banda e protocolo de segurança usado [Ward 2002]. O símbolo em forma de dois semicírculos virados representa uma rede aberta, onde é possível acessar a internet livremente. O círculo fechado representa uma rede fechada sem conectividade. Já o símbolo de um "W" circunscrito representa uma rede com criptografia WEP.

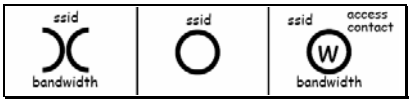

Figura 2. Símbolos *Warchalking* [Ward 2002].

3.7. Vulnerabilidades do WEP e WPA

O *Wired Equivalent Privacy* (WEP), inicialmente especificado no IEEE 802.11 como único protocolo de segurança, teve como objetivo proporcionar um nível de confidencialidade que pudesse ser comparado à rede de cabo estruturado [Douligeris e Serpanos 2007]. Esse protocolo faz uso do algoritmo RC4, criado por Ronald L. Rivest, e implementa a criptografia na camada de enlace. Por padrão, é especificado uma chave de 64 bits, sendo 40 bits para a chave secreta e 24 bits para o vetor de inicialização. No entanto, alguns fabricantes implementam esse algoritmo com chave de 128 bits [Karmakar e Dooley 2008]. Já o *Wi-Fi Protected Access* (WPA), introduzido em dezembro de 2002 com a terceira versão de rascunho do IEEE 802.11i, teve como objetivo resolver as vulnerabilidades presentes no WEP através da atualização de software, não sendo necessário assim a troca do *hardware* [Khadraoui e Herrmann 2007].

A vulnerabilidade do WEP está na forma como o RC4 foi implementado, independente do tamanho da chave adotada [Fluhrer, Mantin e Shamir 2002]. Dentre os vários problemas de segurança podemos destacar: a) As chaves secretas devem ser configuradas manualmente em cada cliente, não havendo um mecanismo para distribuição automática [Karmakar e Dooley 2008]. Isso torna o processo de troca das chaves, recomendado por políticas de segurança, extremamente trabalhoso e raramente feito pelos administradores de rede de grande porte. b) O vetor de inicialização, que além de ser enviado sem criptografia no pacote, é considerado relativamente curto para o seu propósito [Karmakar e Dooley 2008]. Utilizando a técnica de *Scanning* e coletando aproximadamente 300 pacotes, é possível quebrar essa chave [Douligeris e Serpanos 2007]. A ferramenta *AirSnort* [Hegerle e Bruestle 2005], desenvolvida a partir de pesquisas feitas por Tim Newsham, é uma das aplicações que pode ser adotada para esse fim [Mcclure, Scambray e Kurtz 2005].

Já com relação ao WPA, é possível explorar uma tendência que as pessoas têm em escolher senhas fáceis de lembrar [Cache e Liu 2007]. Neste caso, é possível implementar um ataque à chave pré-compartilhada (*Pre-Shared Key* - PSK) com base em um dicionário, usando ferramentas como a *Cowpatty* [Wright 2006] por exemplo. Outra vulnerabilidade

[4] *Service Set Identity* é um valor alfanumérico utilizado para identificar as diferentes WLAN.

está no *Temporal Key Integrity Protocol* (TKIP), que é o protocolo responsável pela troca da chave a cada novo pacote transmitido. Segundo [Moen, Raddum e Hole 2006], capturando alguns pacotes RC4 é possível descobrir a *Temporal Key* (TK) e o *Message Integrity Check* (MIC). Com isso, a complexidade temporal para a quebra da chave RC4 diminui consideravelmente, de 2^{128} para 2^{105}, se comparada ao método de força bruta. Essa vulnerabilidade não representa um risco real à integridade do WPA, no entanto é de grande relevância.

4. Metodologia Proposta

Como mencionado na Introdução, não existe hoje uma metodologia formalizada e genérica para auditar redes 802.11b/g. Essa lacuna faz com que profissionais de segurança da informação tenham extremas dificuldades para identificar vulnerabilidades em suas redes *wireless*, como por exemplo, um *Rogue AP*. Nesse contexto, esboçou-se uma metodologia para auditar redes sem fio, buscando suprir essa necessidade atual.

A metodologia proposta teve como base as seis grandes fases de uma auditoria, abordadas na seção 2. A idéia central dessa metodologia está baseada no fluxograma representado na Figura 3 (versão ainda parcial), na qual cada fase se desdobra em uma série de atividades, as quais estão brevemente explicadas abaixo.

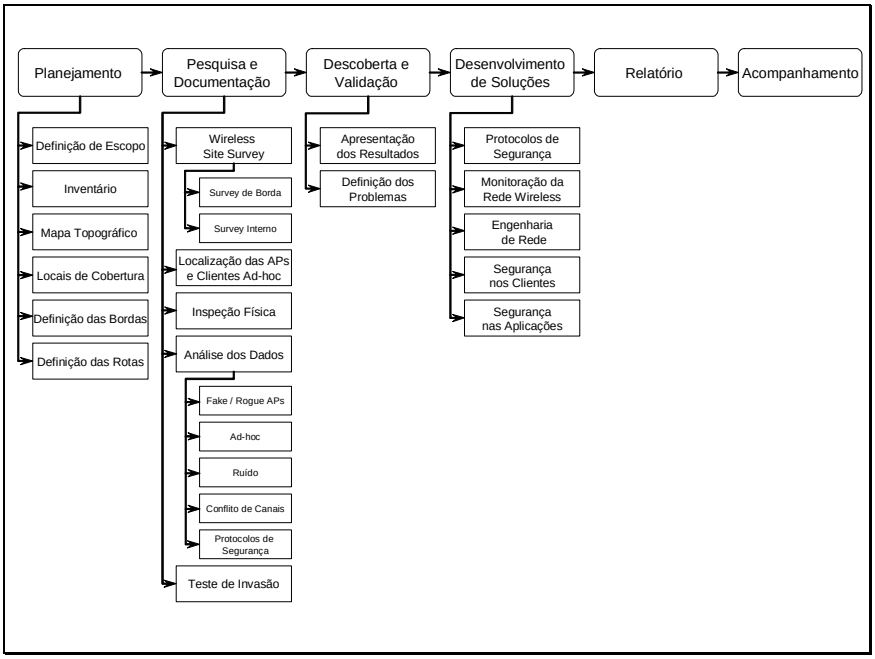

Figura 3. Fluxograma da Metodologia Proposta (versão parcial).

Planejamento:

- Definição de Escopo: descrição dos objetivos da auditoria;
- Inventário: elaboração de em uma planilha contendo todos dos dispositivos *wireless* oficiais e suas características;

● Mapa Topográfico: elaboração de um desenho, preferencialmente com o auxílio de ferramentas de CAD (*Computer-Aided Design*[5]), contendo o leiaute em escala do local onde a auditoria será feita;

● Locais de Cobertura: seleção no mapa topográfico dos locais oficiais de cobertura *Wi-Fi*;

● Definição de Bordas: seleção no mapa topográfico dos limites da área objetiva definida no escopo;

● Definição das Rotas: desenhos no mapa topográfico dos percursos para as coletas de dados.

Pesquisa e Documentação:

● *Wireless Site Survey*: este é o termo usado para coleta de dados durante uma auditoria. Consiste em usar ferramentas do tipo *Scanning* ou *Sniffer* para capturar, e posteriormente analisar, os dados trafegados na rede *wireless*.

● *Survey* de Borda: capturar os dados ao longo das bordas definidas no planejamento;

● *Survey* Interno: capturar os dados ao longo das rotas definidas no planejamento.

● Localização das APs e Clientes *Ad-hoc*[6]: localizar fisicamente todas as APs e os clientes *Ad-hoc* identificados no *survey*. Representá-los graficamente no mapa topográfico, incluindo suas áreas de cobertura;

● Inspeção Física: para cada AP localizado, inspecionar suas condições físicas de instalação. Observar ainda o posicionamento e o tipo da antena. Comparar com os dados registrados no inventário;

● Análise dos Dados: nesta etapa serão analisados os dados coletados durante o site *survey*:

● *Fake* / *Rogue APs*: verificar se um mesmo AP foi encontrado mais de uma vez utilizando canais diferentes, caracterizando um *Fake AP*. Relacionar todos os APs encontrados que não estão presentes no inventário, sendo estes os *Rogue APs*;

● *Ad-hoc*: verificar se os clientes *Ad-hoc* estão presentes no inventário, e ainda, constatar a real necessidade de negócio para o uso dessa topologia;

● Ruído: identificar as áreas e os canais onde há a presença de ruídos. Um estudo mais detalhado pode ser necessário para descobrir a origem precisa desses;

● Conflito de Canais: identificar as áreas de cobertura sobrepostas. Analisar se essas operam no mesmo canal ou em canais muito próximos. Incluir nessa análise os clientes *Ad-hoc*, pois estes também geram conflitos;

● Protocolos de Segurança: classificar os APs e clientes *Ad-hoc* em dois grupos: com e sem configuração de protocolos de segurança, como o WEP

[5] *Computer-Aided Design* são *softwares* utilizados para facilitar o projeto e desenho técnico.

[6] *Ad-hoc* é uma topologia de rede utilizada para conexão ponto a ponto entre dois ou mais clientes *wireless*..

por exemplo. Para o primeiro grupo, identificar os diferentes tipos de mecanismos de segurança, como por exemplo WPA, TKIP, AES, entre outros.

● Teste de Invasão: este tem como objetivo testar os mecanismos de segurança adotados. O teste consiste em explorar as vulnerabilidades conhecidas dos diferentes protocolos.

Descoberta e Validação:

● Apresentação dos Resultado: com base nas análises de dados e no teste de invasão, apresentar os resultados obtidos;

● Definição dos Problemas: a partir dos resultados apresentados, definir quais itens representam um problema real para a necessidade de negócio. Esses serão tratados na etapa seguinte.

Desenvolvimento de Soluções:

● Protocolos de Segurança: empregar os mecanismos de segurança definidos no IEEE 802.11i, como o *Radius*, por exemplo;

● Monitoração da Rede *Wireless*: implementar ferramentas de monitoração no ambiente *wireless*, tais como: a) *Distributed Wireless Security Auditor* - DWSA; b) *Wireless Intrusion Detection Systems* - WIDS; e c) *Radio Monitoring*;

● Engenharia de Rede: Adotar práticas de segurança simples como: a) uso de *Firewall* entre a rede *wireless* e a rede estruturada; b) segmentar a rede em VLANs e controlar o roteamento entre elas; e c) manter desabilitado os pontos de rede sem uso;

● Segurança nos Clientes: aumentar o nível de segurança dos clientes, com ações do tipo: a) habilitar o uso de *Firewall*; b) proibir o uso de redes *Ad-hoc*; c) limitar as conexões *wireless* proibindo *throughputs* menores que 6Mbps ou -90bBm; e d) adotar políticas de atualizações de *software*;

● Segurança nas Aplicações: garantir que as aplicações críticas as necessidades de negócio, ou ainda, as que manipulam dados sensíveis, implementem criptografia em sua camada. O uso de *Transport Layer Security* (TSL) ou *Security Sockets Layer* (SSL) são exemplos de criptografia para a camada de aplicação.

5. Conclusões e Trabalhos Futuros

As dificuldades enfrentadas por profissionais responsáveis pelo suporte de ambientes *wireless* são reais, bem como as inúmeras vulnerabilidades existentes no IEEE 802.11. A especificação de uma metodologia para auditoria dessas redes sem fio é de extrema relevância no contexto atual. Contudo, o presente artigo representou uma parcela inicial da pesquisa ainda em andamento, e na qual é esperada uma conclusão definitiva para dezembro de 2008.

Para as próximas atividades dessa pesquisa, estão previstas: a) detalhamento ao nível de execução das atividades do método proposto; b) especificação das atividades dos itens de Relatório e Acompanhamento; c) análise de estudo de caso; e d) aplicação da metodologia no caso estudado.

Referências

Cache, J. e Liu, V. (2007) “Hacking Exposed Wireless: Wireless Security Secrets & Solutions”, Books24x7: McGraw-Hill/Osborne.

CISCO (2007) “Cisco Vaults Over 4 Million Wireless Access Points Milestone”, San Jose: Press Release, Disponível em: <http://newsroom.cisco.com/dlls/2007/prod_040207.html>, Acessado em: março 2008.

Davis, C., Schiller, M. e Wheeler, K. (2007) “IT Auditing: Using Controls to Protect Information Assets”, Books24x7: McGraw-Hill.

Douligeris, C. e Serpanos, D. N. (2007) “Network Security: Current Status and Future Directions”, Books24x7: IEEE Press.

Fluhrer, S., Mantin, I. e Shamir, A. (2002) “Attacks on RC4 and WEP”, Israel: Weizmann Institute, Disponível em: <http://www.wisdom.weizmann.ac.il/mathusers/itsik/RC4/Papers/rc4_wep.ps>, Acessado em: maio 2008.

Hegerle, B. e Bruestle, J. (2005) “AirSnort”, Disponível em: <http://airsnort.shmoo.com>.

Hewlett-Packard (2008) “HP Network Node Manager (NNM) Advanced Edition software”, Disponível em: <http://www.openview.hp.com/products/nnm/index.html>.

Hurley, C. (2007) “WarDriving & Wireless Penetration Testing”, Books24x7: Syngress.

INCISOR (2007) “Are Consumers Getting the Message”, Hampshire: Click I.T. Ltd, Disponível em: <http://www.incisor.tv/pdf/108may2007.pdf>, Acessado em: março 2008.

Karmakar, G. e Dooley, L. S. (2008) “Mobile Multimedia Communications: Concepts, Applications, and Challenges”, Books24x7: IGI.

Kershaw, M. (2008) “Kismet”, Disponível em: < http://www.kismetwireless.net >.

Khadraoui, D. e Herrmann, F. (2007) “Advances in Enterprise Information Technology Security”, Books24x7: IGI.

Mcclure, S., Scambray, J. e Kurtz, G. (2005) “Hacking Exposed: Network Security Secrets & Solutions”, Books24x7: McGraw-Hill/Osborne, Fifth Edition.

Miyoshi, E. M. e Sanches, C. A. (2002) “Projetos de sistemas rádio”, São Paulo: Érica.

Moen, V., Raddum, H. e Hole, K. J. (2006) “Weaknesses in the Temporal Key Hash of WPA”, Disponível em: < https://bora.uib.no/bitstream/1956/1901/21/Paper_4_Moen.pdf>.

Ward, M. (2002) “Write here, right now”, London: BBC News, Disponível em: <http://news. bbc.co.uk/1/hi/in_depth/sci_tech/2000/dot_life/2070176.stm>, Acessado em: abril 2008.

Wright, J. (2006) “coWPAtty”, Disponível em: <http://wirelessdefence.org/Contents/coWPAttyMain.htm>.