Site survey: mapeamento, detecção de vulnerabilidades e análise de sinal de redes sem fio

William Carlos de J. Rodrigues
Graduado em Ciência da Computação – Uninove.
São Paulo – SP [Brasil]
william@pantechbrasil.com.br
wi_rodrigues@hotmail.com

Ezequiel Ferreira dos Santos
Professor na Graduação [Ciência da Computação] – Uninove.
São Paulo – SP [Brasil]
efsantos@uninove.br

A técnica do *site survey* em redes *wireless* possibilita o mapeamento gráfico, a análise de sinais *wi-fi* e a detecção de vulnerabilidades em redes sem fio. O conhecimento dessa ferramenta é fundamental para determinar a viabilidade de sua implantação e analisar a abrangência dos sinais de radiofreqüência, contribuindo para a execução de projetos de redes *wireless*, com qualidade, eficiência e segurança.

Palavras-chave: Redes. *Site survey*. *Wi-fi*. *Wireless*.

1 Introdução

Uma importante fase de qualquer projeto de implantação de redes *wireless* é o *site survey*, uma técnica que utiliza ferramentas para analisar a qualidade dos sinais de transmissão e os ruídos, entre outras opções de sinais de redes, e que, no entanto, não é explorada no Brasil.

A maioria das organizações que possuem ou pretendem implantar redes sem fio enfrenta muitos problemas relacionados à conectividade, à baixa qualidade de sinais de transmissão e às invasões de *hackers*. Esses obstáculos exigem competência cada vez maior para administrar redes *wireless*, à medida que essa tecnologia evolui.

Neste trabalho, tem-se por objetivo apresentar uma forma de mapeamento gráfico, análise de sinais *wi-fi* e detecção de vulnerabilidades em redes sem fio, por meio da técnica do *site survey* em redes *wireless*.

2 Os padrões *wi-fi* 802.11 a, b e g.

O Institute of Electrical and Electronics Engineers (IEEE) criou um comitê organizador para definir todos os padrões de comunicação em redes sem fio, denominados 802.11, também conhecidos como *wi-fi*. Nos últimos anos, houve grande disseminação dessa tecnologia, tendo sido especificados padrões que formam a arquitetura 802.11x, destacando-se:

- 802.11a: com freqüência de operação de 5 GHz, permite que 64 clientes se conectem a WEP (*Wired Equivalent Privacy*) de 256 bits, por meio da utilização do tipo de modulação OFDM (*Orthogonal Frequency Division Multiplexing/Modulation*). A principal restrição desse padrão é a falta de compatibilidade com os outros padrões b e g, devido à utilização de diferentes faixas de freqüência (RUFINO, 2005);
- 802.11b: utiliza freqüência de 2,4 GHz com tipo de modulação DSSS (*Direct Sequence Spread Spectrum*) e permissão máxima de 32 clientes conectados (RUFINO, 2005);
- 802.11g: atua na freqüência de 2,4 GHz, com a possibilidade de equipamentos de ambos os padrões – b e g – coexistirem no mesmo ambiente. A velocidade de transmissão pode chegar a 108 Mbps com a utilização de recursos de compactação de dados e modulação do tipo OFDM (RUFINO, 2005).

3 *Access points* e antenas

Os APs (*access points*, Dispositivos Concentradores ou Transmissores de Sinais) são, entre todos os dispositivos existentes nas redes *wireless*, os que possuem maior funcionalidade. Esses equipamentos são responsáveis pela distribuição de sinais e centralização de redes, de modo que todas as conexões firmadas em uma rede sejam dependentes da intensidade do sinal de radiofreqüência (RF) gerado pelo AP.

Os *access points* podem ser classificados, inicialmente, em duas categorias:

AP *indoor*: popular e de custo relativamente baixo, é geralmente utilizado em ambientes fechados que não necessitam de um amplo sinal de cobertura direcional. O sinal de radiofreqüência transmitido por esse tipo de equipamento abrange uma área circular, em decorrência da utilização de antenas do tipo Omni, com raio de aproximadamente 100m, em ambientes que não apresentam muitos obstáculos que poderiam diminuir, substancialmente, esse valor. A intensidade do sinal gerado pelo AP *indoor* pode variar de 16 a 18 dBm, dependendo da potência das antenas utilizadas.

AP *outdoor*: de uso restrito e custo relativamente alto, é utilizado em ambientes abertos e instalações que necessitam de maior potência de sinais de transmissão. Operam com antenas do tipo Omni ou Direcionais e podem transmitir sinais de radiofreqüência com potências variáveis entre 19 e 28 dBm, dependendo do tipo de antena utilizada. Além dessas funcionalidades, esses APs podem trabalhar nos modos ponto-a-ponto, para interligar duas redes localizadas em diferentes prédios, ou ponto-a-multiponto, semelhante ao esquema de infra-estrutura de redes *wi-fi*, em que um AP central, que utiliza antenas do tipo Omni, estabelece conexão com outros APs que adotam antenas direcionais (JARDIM, 2005).

4 Segurança em redes *wireless*

Pelo fato de redes sem fio possuírem menores limitações geográficas, os riscos associados aos aspectos físicos envolvidos são maiores (GAVRILENKO et al., 2004). Administradores de redes *wireless* tendem a se preocupar muito mais com a segurança lógica em detrimento da física, o que é um grave erro, visto que a área de abrangência física de redes sem fio aumenta substancialmente quando o meio de propagação do sinal é o próprio ar. Hoje, os padrões mais utilizados em implantações de redes *wireless* são o 802.11b e 802.11g, que possuem sinais com alcance muito maior que os do padrão 802.11a, devido à potência dos equipamentos de transmissão que, atualmente, chegam a 300 mV. Por essas características, um teste de propagação de sinal não deve ser o único fator de prevenção a ataques.

Não se deve ignorar o fato de vários mecanismos de segurança modernos não estarem habilitados pelo fabricante. Além de chegarem aos usuários com endereço IP (Internet Protocol) e senha de administração padrão, esses equipamentos possuem um serviço chamado SNMP (*Simple Network Management Protocol*), responsável pelas informações gerenciais sobre o aparelho e o respectivo tráfego. Se essas configurações de fábrica não forem alteradas, poderão prover conexão livre para *hackers*.

4.1 *Softwares* e técnicas utilizadas nos ataques dos *hackers*

Há alguns exemplos já conhecidos de *softwares* e técnicas utilizados por *hackers* em ataques a redes *wireless*.

O *Airtraf* consiste em um programa que coleta diversas informações sobre uma rede sem fio detectada, tais como a quantidade de clientes conectados e de serviços utilizados. Existe também o BSD (*Berkeley Software Distribution*) *AirTools*, utilizado para capturar pacotes que possibilitem a quebra de chaves WEP, embora apresentem diversos tipos de incompatibilidade em relação a interfaces de rede e padrões (PROJECTS, 2004). Uma das ferramentas mais poderosas no que se refere ao número de funcionalidades é o *Kismet*, que possui módulos de mapeamento de redes, captura de tráfego, monitoramento, visualizador de *logs*, entre outros, o que o torna uma ferramenta muito útil nas mãos de *hackers* (KERSHAW, 2007). O *AirJack*, um *software* bem simples, possibilita ao invasor fazer-se passar por um dispositivo concentrador (*access point*) para obter informações de possíveis clientes que venham a conectar-se (LYNN, 2005).

Entre os *softwares*, o mais famoso é o *Ethereal*, que, em termos de captura de pacotes, é um dos mais completos e com maior número de funcionalidades, tais como as possibilidades de remontar uma seção, de selecionar um tráfego por campos (cabeçalhos, origem, destino, tipo de protocolo, porta etc.) e de tratar pacotes específicos de redes *wireless* (LESKO, 2001).

Para quebras de chaves WEP, há grande variedade de *softwares* que, entre outras ferramentas desse tipo, implementam o ataque à geração de chaves fracas, baseando-se nos termos do Fluhrer, Mantin, and Shamir (FMS) *attack* ou ataques do tipo dicionário (RUFINO, 2005).

5 Site survey

Por definição, *site survey* é um conjunto de métodos aplicados na avaliação técnica minuciosa do local de instalação de uma nova infra-estrutura de rede *wireless*, na observação dos resultados obtidos dos *upgrades* de uma infra-estrutura já utilizada ou, até mesmo, na detecção e resolução de possíveis problemas em um sistema ativo.

Esses processos são efetuados, normalmente, durante o estudo de viabilidade do projeto, seja no levantamento da infra-estrutura necessária (dispositivos de conectividade, transmissores, concentradores, acessórios etc.), ou na instalação de uma nova rede estruturada, de equipamentos transmissores de radiofreqüência e redes *wireless*. O objetivo é realizar um estudo sobre esses recursos para entender seu comportamento, descobrir áreas cobertas, checar interferências de radiofreqüência, indicar a disposição apropriada dos dispositivos *wireless*, determinar o melhor aproveitamento do local estudado quanto à cobertura e eficiência de sinais, bem como em relação à redução dos custos de investimento.

Existem conceitos referentes às áreas de cobertura de redes *wireless*, considerados como topologias básicas. Cada área coberta por sinais de RF irradiados por um único dispositivo transmissor é chamada de Área de Serviço Básica (*Basic Service Area* [BSA]), também conhecida como célula (JARDIM, 2005).

O *access point* central da rede se comunica com todos os aparelhos *wireless* na área da BSA e controla todo o fluxo de tráfego da rede. Os aparelhos remotos não se comunicam diretamente uns com os outros; por isso, precisam do AP para estabelecer conexão.

Se uma única BSA não produzir cobertura suficiente para todos os dispositivos da rede, qualquer quantidade de células poderá ser adicionada para aumentar a abrangência da cobertura de sinais. Esse grupo de BSAs é conhecido como uma Área de Serviço Estendida (Extended Service Area – ESA). É recomendado que as BSAs de uma ESA tenham de 10 a 15% de sobreposição para permitir que usuários remotos naveguem sem perda de conexão e com garantia de cobertura de sinal de RF. As BSAs que fazem fronteira umas com as outras devem ser colocadas em diferentes canais de transmissão para obtenção de melhor desempenho.

Em uma rede *wireless*, problemas podem impedir que o sinal de RF alcance todas as partes de uma área. Vários fatores poderão causar interferências de sinal, tais como:

- Distorção multidirecional (mais conhecida como distorção *multipath*);
- Posição dos pontos de acesso;
- Clientes de 802.11b em uma célula de 802.11g;
- Reutilização do canal;
- Facilidades adjacentes;
- Posição das antenas em um *laptop*;
- Posição dos cristais na placa-mãe do *laptop*;

O problema encontrado com maior freqüência é a distorção multidirecional causada por reflexões de rádio. Quanto mais alto o número de sinais de radiofreqüência na célula, mais alto será o nível de ruído dentro dela. Portanto, as antenas de *access points* devem estar dispostas longe das superfícies reflexivas, de objetos metálicos ou fora de fase.

Para solucionar esses problemas, é preciso localizar sua ocorrência. O *site survey* facilita a definição das linhas de radiofreqüência cobertas em um determinado espaço e possui recursos que são utilizados para descobrir regiões em que a distorção *multipath* pode ocorrer – áreas em que a interferência de RF é alta – e disponibilizar soluções para eliminar esses obstáculos. Um *site survey* que determina a área de cobertura de RF também ajuda a escolher um número de dispositivos. (WIRELESS, 2006).

Podemos classificar o *site survey* em duas categorias:

> *Site survey indoor*: consiste em realizar a inspeção de redes *wireless*, buscando interferências, localização de *access points* e disposição geográfica de dispositivos em BSAs. Esse tipo de inspeção fornece gráficos de intensidade de sinais mais fáceis de serem analisados, visto que as pesquisas são realizadas em espaços relativamente pequenos. Geralmente, efetuado em projetos ou redes menores que não possuem interligação entre diferentes áreas geográficas, esse tipo de pesquisa pode ser feito de dois modos nos ambientes fechados – *mono* ou *multifloor* (em um ou mais andares). As fontes de interferências são menores nesses ambientes, o que facilita a escolha de antenas e dispositivos transmissores e receptores (GEIER, 2002).

Site survey outdoor: consiste em realizar a inspeção de redes *wireless* em um âmbito muito maior que o existente na modalidade *indoor*, por meio de interferências mais complexas. Busca-se determinar a localização e posição de *access points* e das antenas de transmissão de grande porte, com base na disposição geográfica dos dispositivos das ESAs e dos demais aspectos de inspeção do *site survey*. Essa modalidade de inspeção fornece gráficos de cobertura de sinais de radiofreqüência cuja análise é mais complexa, em face das inúmeras variações que ocorrem em razão do grande número de fontes de interferências externas que existem em amplos espaços geográficos. Geralmente, é realizado em projetos ou redes de grande porte que possuem diversas interligações com diferentes redes localizadas em áreas distantes. Deve-se levar em consideração interferências eletromagnéticas, elétricas, a diversidade de antenas de transmissão e o elevado número de ondas de radiofreqüência de distintas tecnologias, tais como rádios, celulares e emissoras de TV, para se efetuar a inspeção minuciosa dos sinais de redes *wireless* e a análise correta dos resultados obtidos (GEIER, 2002).

Os procedimentos envolvidos na metodologia *site survey* visam dimensionar adequadamente o local de instalação dos equipamentos transmissores e receptores de sinais de RF, para que todas as estações possam desfrutar de qualidade nas conexões, tendo total acesso às aplicações disponíveis na rede. Para tanto, faz-se necessário executar um conjunto de etapas específicas, que vão desde a aquisição de equipamentos à realização dos passos necessários à obtenção de resultados (PINHEIRO, 2004). Alguns dos equipamentos básicos, essenciais à implementação de um *site survey,* incluem:

- Ponto de acesso *wireless*;
- Cartão de cliente *wireless* (NIC);
- Laptop ou PDAs;
- Antenas variadas (dependendo da necessidade e do escopo do projeto a ser implementado);
- *Software* de utilitários do *site survey*.

Uma vez com esses equipamentos, deve-se executar os seguintes passos para montar um *site survey* adequadamente:

- Reunir mapas ou plantas dos locais a serem inspecionados;
- Configurar o *software* de acordo com o funcionamento da interface de rede *wireless* a ser utilizada;
- Realizar uma pré-análise visual do local a ser inspecionado;
- Percorrer o local por completo durante a captura de sinais de radiofreqüência, para certificar-se da precisão dos resultados;
- Reunir os resultados obtidos e dispô-los em diagramas comparativos dos itens inspecionados.

Atualmente, muitas empresas têm investido em novas tecnologias aplicadas em redes *wi-fi* (como o *site survey*, por exemplo), tanto comercialmente quanto na comunidade acadêmica, fornecendo cursos e novas certificações. No entanto, devido à pouca difusão dessas tecnologias no Brasil, profissionais da área e interessados em sua aquisição são ainda obrigados a buscar opções no exterior (GEIER, 2002).

6 *Site Survey Outdoor* – Experimento

O experimento realizado consistiu em aplicar, na prática, métodos e ferramentas do *site survey*, do tipo *outdoor*, adotando como área de cobertura os arredores da Avenida Paulista, alvo de muitos ataques *wireless* de *hackers*, dado o imenso número de redes sem fio existentes. O local exato escolhido para aplicação abrangeu, na seqüência, a Alameda Campinas, a Rua São Carlos do Pinhal e a Rua Pamplona.

A operação ocorreu em um fim de semana, mais precisamente no sábado, dia 29 de julho de 2006, no intervalo das 12 às 13 horas, por supor-se que, na data e no horário mencionados, existiriam menos clientes conectados, o que facilitaria a detecção de redes e suas conexões. Isso por objetivar-se a coleta de informações de caráter acadêmico para este projeto.

7 Metodologia

Para a realização do experimento em questão, foram utilizados um notebook, com interface de rede *wi-fi* compatível com os padrões 802.11 B e G, um *software* específico para a aplicação do *site survey*, um veículo e um inversor de corrente elétrica DC/AC. Foram ainda pesquisados e reunidos mapas, fotos e imagens de satélite dos possíveis locais a serem explorados. Além disso, avaliou-se a viabilidade de acesso a acostamentos e prédios que possuiriam equipamentos transmissores de sinais de radiofreqüência e antenas de transmissão propriamente ditas.

Inicialmente, foi efetuada a configuração do *software* de captura de sinais, no qual foi carregado o mapa do local selecionado bem como configurados os *drivers* do *hardware* de captura para dar início aos métodos de análise e detecção de sinais.

O local designado foi percorrido, lentamente, a uma velocidade média de 30 km/h, com sucessivas paradas a cada 30 segundos, para melhor fixação e interpretação do local a ser verificado pelo *software*. Esse processo foi repetido até que todo o caminho tivesse sido completado para, só então, reunir as imagens dos resultados obtidos.

Após detecção e análise dos sinais de radiofreqüência, o processo de captura de imagens geradas pelo *software* foi iniciado. A partir da rea-

lização satisfatória do *site survey outdoor* e da análise dos resultados obtidos, observou-se que algumas redes possuíam sinais de radiofreqüência muito fortes. Em seguida, o percurso foi efetuado uma terceira vez, com o intuito de se conectar às redes identificadas.

8 Resultados

A aplicação do *site survey outdoor* possibilitou obter sinais de radiofreqüência de 16 redes *wireless*, diagramas com informações detalhadas sobre cada uma delas, com definição do canal de freqüência em que cada uma atua. Outros dados foram a intensidade do sinal de cada rede, ilustrada, graficamente, em mapas ou gráficos que relacionam intensidade de sinal e tempo de inspeção; a relação sinal/ruído ilustrada no mapa; o provável local em que se encontra o dispositivo transmissor (*access point* ou Antena) e o tipo de ferramenta de segurança implementada em cada uma, entre outros.

Durante a avaliação, foram detectadas precisamente 16 SSIDs (*Service Set Identifiers*) de redes *wireless*, listadas automaticamente na tela de captura do *software*; algumas com nomes sugestivos de redes domésticas e outras com nomes prováveis de redes corporativas. Ao contrário do previsto, quase todas as redes detectadas apresentavam algum tipo de mecanismo de segurança habilitado, seja por chave de acesso com criptografia, seja por servidor de autenticação de usuários, o que demonstra certa evolução da tecnologia *wi-fi*.

Foram constatadas muitas variações de sinais de radiofreqüência, entre as quais, redes com sinais potentes e algumas com vestígios de sinais. Os sinais capturados chegaram a um nível máximo de 23 dBm de intensidade, abrangendo uma ampla área de cobertura, provavelmente por estar utilizando equipamentos transmissores potentes, fornecendo, desse modo, plena conectividade aos arredores do local avaliado.

Os gráficos foram criados a partir da intensidade dos sinais de RF, obtidos de posições inseridas no *software* e representados de acordo com uma legenda de cores correspondentes aos respectivos valores de ondas de RF em dBm.

Algumas das redes detectadas apresentaram sinais de transmissão reduzidos, provavelmente, por serem oriundos de redes domésticas, que utilizam *access points* e antenas de baixa potência de transmissão, tornando muito difícil o estabelecimento de uma conexão estável com redes dessa categoria (Figura 1).

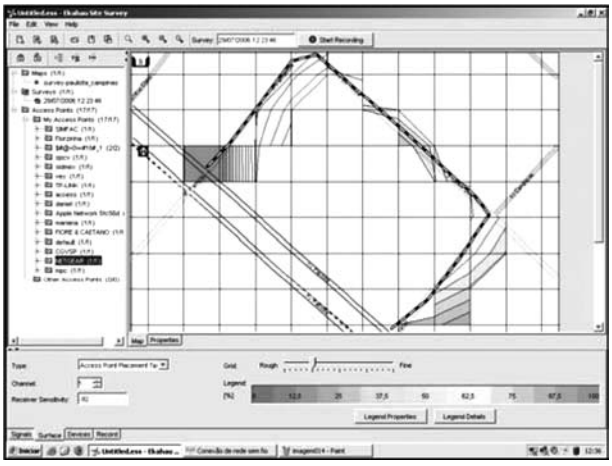

Figura 1: Rede detectada apenas com vestígio de sinais de radiofreqüência

Fonte:

Uma das principais funcionalidades do *software* adotado é o fornecimento de gráficos de intensidade dos sinais durante o tempo de avaliação. Ao longo da aplicação do *site survey*, esses sinais foram capturados e analisados nos gráficos gerados (Gráfico 1), que demonstraram os estados dos sinais de RF em cada horário, no intervalo de tempo em que foi realizada a inspeção. Essa ferramenta facilitou a análise da qualidade de conectividade e a identificação de variações e interferências em potencial, nas ondas de radiofreqüência.

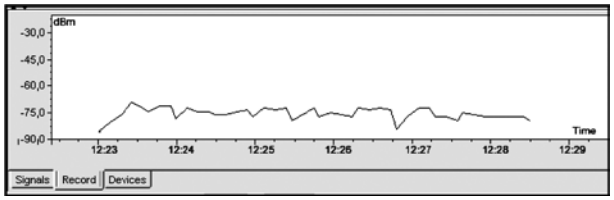

Gráfico 1: Intensidade de sinais de RF em função do tempo

Fonte:

O identificador de localização do dispositivo transmissor de sinal – o *Access Point Location* – é outra funcionalidade que aponta, no mapa, a provável localização do a*ccess point* ou da antena de transmissão, sendo possível determinar os posicionamentos dos dispositivos transmissores de sinais de todas as redes detectadas, o canal de transmissão em que cada uma opera e o padrão de comunicação. Com a definição desses fatores e da freqüência utilizada, pode-se identificar as possíveis fontes de interferência e as áreas diretamente afetadas por elas (Gráfico 2).

Por fim, a última funcionalidade associa-se à geração do gráfico que relaciona sinal e ruído (gráfico SNR), obtido do diagrama completo de informações geradas ao final da avaliação do *site survey* (Gráfico 3). Seguindo a mesma legenda de cores adotada anteriormente, esse gráfico demonstrou o local com interferências externas maiores e mais intensas.

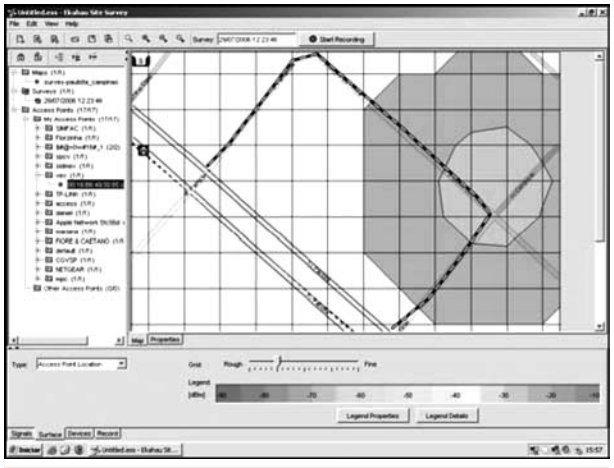

Gráfico 2: Localização do *access point*

Fonte:

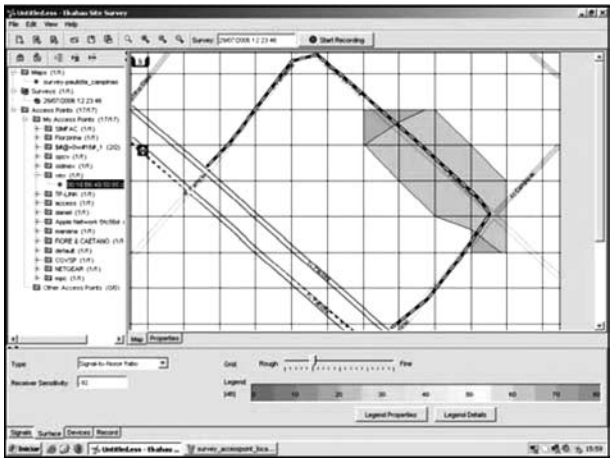

Gráfico 3: Sinal em função do ruído

Fonte:

Verificado o sucesso obtido pela aplicação do experimento sobre o *site survey*, optou-se por mais uma avaliação no local escolhido, porém com o propósito de verificar a segurança das redes detectadas. Aproveitando as informações adquiridas por meio da utilização do *software* de avaliação, foram determinadas as redes com os melhores sinais de transmissão. Na tentativa de conexão, observou-se que a rede-alvo não possuía mecanismo de segurança por criptografia, o que permitiu estabelecer conexão, obter automaticamente endereços IP por DHCP (*Dynamic Host Configuration Protocol*) e, a partir dos comandos "ipconfig" e "ping", descobrir o endereço do *gateway* e verificar sua conectividade. Assim, foi possível conectar-se à página inicial do servidor DHCP, constatando-se que se tratava de uma rede com autenticação RADIUS (Figura 2).

9 Considerações finais

A evolução da tecnologia *wireless* tem-se mostrado cada vez mais intensa, de forma que, a cada dia, surgem novos padrões e equipamentos.

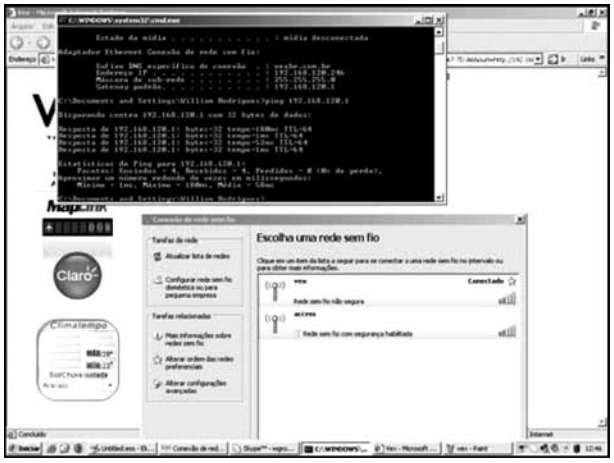

Figura 2: Verificação de conectividade

Fonte:

A realização do *site survey* mostrou-se eficaz porque reuniu informações sobre as ferramentas de segurança utilizadas, a abrangência de determinadas áreas de cobertura de sinais de radiofreqüência das redes, a intensidade desses sinais, demonstrados, detalhadamente, em gráficos e mapas dos locais pesquisados, e a organização da infra-estrutura (localização geográfica dos dispositivos) dessas redes.

Por fornecer todos esses dados, a utilização do *site* colabora para decidir-se sobre novas instalações, *upgrades*, seleção de equipamentos (desde a implantação dos *access points* até o uso de antenas de transmissão de sinais de radiofreqüência) mais apropriados a ambientes específicos ou de melhor adaptação a determinadas instalações. Forneceu, ainda, informações relevantes sobre investimentos em técnicas e mecanismos, para se adotar em novas políticas de segurança de acesso a dados ou conectividade. Contribui ainda para a documentação de redes *wireless*, que, apesar de ser de extrema importância para o administrador, não é encontrada facilmente. Ressalta-se, por fim, que a principal vantagem do *site survey* consiste na possibilidade de alterar os custos investidos em um determinado projeto como a realização de uma análise de melhor posicionamento dos *access points* de uma rede, com a pretensão de reduzir o número desse equipamento, impactando no valor total do projeto.

As informações obtidas neste estudo são relevantes, levando-se em consideração a atual necessidade de segurança, economia, alta disponibilidade de informações, conectividade e qualidade de serviços com que nos deparamos.

Site survey: mapping, detection of vulnerabilities and analysis of nets wireless signal

The technique of the site survey in wireless networks makes possible the graphical mapping, the analysis of wi-fi signals and the detection of vulnerabilities in wireless networks. The acquaintance with this tool is essential to determine the viability of its implantation and to analyze radio frequency signals, collaborating to the execution of wireless networks projects with quality, efficiency and security.

Key words: Nets. Site survey. Wi-fi. Wireless.

Referências

JARDIM, F. de M. *Guia profissional de redes Wireless:* Voip/Wi-fi/Bluetooth/Wimax/Infravermelho/ Skype. 1. ed. São Paulo: Digerati Books, 2005.

GEIER, J. *Site survey tools simplify 802.11 deployments*. 2002. Disponível em: <http://www. *wi-fi*planet.com/tutorials/article.php/953661>. Acesso em: 10 mar. 2006.

GEIER, Jim. *RF site survey steps*. 2002. Disponível em: <http://www.*wi-fi*planet.com/ tutorials/article.php/1116311>. Acesso em: 10 mar. 2006.

GAVRILENKO, K. V.; MIKHAILOVSKY, A. A; VLADIMIROV, A. A. *Wi- foo*: the secrets of *wireless* hacking. 1. ed. Boston: Addison-Wesley, 2004.

KERSHAW, K. *Kismet Readme*. 2007. Disponível em: <http://www.kismetwireless.net/documentation. shtml>. Acesso em: 18 ago. 2006.

LESKO, M. Ethereal. *Sys Admin*, Boulder, v. 10, n. 11, nov. 2001. Disponível em: <http://www.samag.com/documents/s=1441/sam0111a/0111a.htm>. Acesso em: 25 ago. 2006.

LYNN, M. *AirJack*. 2005. Disponível em: <http://www.wirelessve.org/entries/show/WVE-2005-0018>. Acesso em: 4 ago. 2006.

PINHEIRO, J. M. S. *Site survey*: o segredo de um bom projeto. 2004. Disponível em: <http://www.projetoderedes.com.br/artigos/artigo_*wireless_survey*.php>. Acesso em: 23 mar. 2006.

PROJECTS: bsd-airtools v0.2. 2004. Disponível em: <http://www.dachb0den.com/projects/bsd-airtools.html>. Acesso em: 27 jul. 2006.

RUFINO, N. M. de O. *Segurança em redes sem fio*: aprenda a proteger suas informações em ambientes *wi-fi* e *bluetooth*. 1. ed. São Paulo: Novatec, 2005.

WIRELESS site survey FAQ. 2006. Disponível em: <http://www.cisco.com/en/US/tech/tk722/ tk809/technologies_q_and_a_item09186a00805e9a96.shtm>. Acesso em: 2. abr. 2006.

Recebido em 13 dez. 2007 / aprovado em 2 maio 2007

Para referenciar este texto

RODRIGUES, W. C. de J.; SANTOS, E. F. de. *Site survey*: mapeamento, detecção de vulnerabilidades e análise de sinal de redes sem fio. *Exacta*, São Paulo, v. 5, n. 1, p. 69-78, jan./jun. 2007.