

LIGA DE ENSINO DO RIO GRANDE DO NORTE  
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RIO GRANDE DO  
NORTE  
BACHARELADO EM SISTEMAS DE INFORMAÇÃO

**ESTUDO DE CASO DA REDE WIRELESS DE UMA INSTITUIÇÃO DE ENSINO**

**Alessandro Andreole da Cunha Oliveira**

NATAL/RN  
2010

**ALESSANDRO ANDREOLE DA CUNHA OLIVEIRA**

**ESTUDO DE CASO DA REDE WIRELESS DE UMA INSTITUIÇÃO DE ENSINO**

Monografia apresentada ao curso de Graduação em Bacharelado em Sistemas de Informação da Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte para obtenção do grau de Bacharel em Sistemas de Informação.

**Orientador:**

Romulo Fagundes Catanhede (Esp.)

NATAL/RN  
2010

LIGA DE ENSINO DO RIO GRANDE DO NORTE  
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RIO GRANDE DO  
NORTE  
CURSO DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO

**ESTUDO DE CASO DA REDE WIRELESS DE UMA INSTITUIÇÃO DE ENSINO**

**Alessandro Andreole da Cunha Oliveira**

Monografia apresentada e aprovada em \_\_\_\_ de \_\_\_\_\_ de \_\_\_\_, pela banca examinadora composta pelos seguintes membros:

---

Prof. Romulo Fagundes Catanhede (Esp.)  
Orientador

---

Prof. Aluizio Ferreira da Rocha Neto (Msc.)  
Membro Examinador

---

Prof. Luiz Gonzaga Damasceno (Msc.)  
Membro Examinador

Natal/RN, \_\_\_\_ de \_\_\_\_\_ de \_\_\_\_.

À minha família dedico este trabalho, por sempre ter acreditado em minhas capacidades, principalmente ao meu pai, por ter me dado esta grande oportunidade.

À minha namorada, Tainá, que me auxiliou durante este projeto.

## **AGRADECIMENTOS**

Gostaria primeiramente de agradecer a Deus, por sempre ter me colocado no caminho certo.

À meu pai, por ter tornando muitos de meus sonhos possíveis e por ser um exemplo de homem a seguir.

À minha mãe, por ser uma mulher guerreira, batalhadora e por ter me guiado para o lado certo da vida.

À minha namorada, pela paciência ao longo desses cinco anos de namoro, pelo apoio e também pela ajuda neste projeto.

À meu orientador, Romulo Catanhede, por ter depositado uma grande confiança neste estudo, também por suas sugestões, críticas e dicas.

A todos os professores e amigos que, direta ou indiretamente contribuíram para a conclusão deste trabalho.

## **RESUMO**

O projeto apresenta um estudo sobre a realidade da rede Wireless em uma Instituição de Ensino, apontando seus pontos falhos em relação à segurança, gestão de perfis dos usuários, centralização das configurações e equipamentos utilizados. Em cima dos pontos falhos, serão mostradas algumas soluções cabíveis para esta instituição, desta forma melhorando o desempenho e segurança, além de facilitar a gestão da rede.

**Palavras-Chave:** Sem fio. Vulnerabilidade. Segurança.

## **ABSTRACT**

The project presents a study on the reality of the wireless network in an Education Institution, pointing out their defective points in relation to security management, user profiles, centralized configuration and equipment used. On top of missing points, will show some reasonable solutions to this institution, thereby improving performance and security, and facilitate network management.

**Keywords:** Wireless. Vulnerability. Security.

## SUMÁRIO

|                                                           |           |
|-----------------------------------------------------------|-----------|
| <b>1. INTRODUÇÃO.....</b>                                 | <b>9</b>  |
| <b>2. OBJETIVOS .....</b>                                 | <b>10</b> |
| 2.1. OBJETIVO GERAL.....                                  | 10        |
| 2.2. OBJETIVOS ESPECÍFICOS .....                          | 10        |
| <b>3. JUSTIFICATIVA .....</b>                             | <b>11</b> |
| <b>4. REFERENCIAL TEÓRICO .....</b>                       | <b>12</b> |
| 4.1. CRIPTOGRAFIAS.....                                   | 12        |
| 4.1.1. WEP (WIRED EQUIVALENT PRIVACY).....                | 12        |
| 4.1.2. WPA (WI-FI PROTECTED ACCESS).....                  | 13        |
| 4.1.3. WPA2.....                                          | 13        |
| 4.2. VULNERABILIDADES .....                               | 14        |
| 4.2.1. VULNERABILIDADE DA CRIPTOGRAFIA WEP .....          | 14        |
| 4.2.2. MÁ CONFIGURAÇÃO DOS ROTEADORES WIRELESS.....       | 14        |
| 4.2.3. MAC SPOOFING.....                                  | 15        |
| 4.3. SOLUÇÕES WIRELESS .....                              | 15        |
| 4.3.1. AD HOC.....                                        | 15        |
| 4.3.2. REPETIÇÃO DE SINAL.....                            | 16        |
| 4.4. FERRAMENTAS .....                                    | 17        |
| 4.4.1. WARDRIVING .....                                   | 17        |
| 4.4.2. WARCHALKING .....                                  | 18        |
| 4.4.3. AIRSNORT .....                                     | 18        |
| 4.4.4. KISMET.....                                        | 19        |
| 4.4.5. NETSTUMBLER .....                                  | 20        |
| 4.5. SERVIDORES .....                                     | 21        |
| 4.5.1. FIREWALL.....                                      | 21        |
| 4.5.2. DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL) .....   | 23        |
| 4.5.3. KERBEROS .....                                     | 24        |
| 4.5.4. LDAP (LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL) ..... | 26        |
| 4.6. EQUIPAMENTOS.....                                    | 27        |
| 4.6.1. ACCESS POINTS .....                                | 27        |
| 4.6.1.1. ACCESS POINT 3COM .....                          | 27        |
| 4.6.1.2. ROUTERBOARD.....                                 | 28        |
| <b>5. ESTUDO DE CASO .....</b>                            | <b>30</b> |
| 5.1. REALIDADE ATUAL.....                                 | 30        |
| 5.2. REALIDADE PROPOSTA .....                             | 32        |
| 5.2.1. ROUTERBOARD MICROTIK .....                         | 32        |
| 5.2.2. DHCP.....                                          | 32        |
| 5.2.3. PROXY .....                                        | 33        |
| 5.2.4. BLOQUEIO DE COMPARTILHAMENTO .....                 | 34        |
| 5.2.5. GRUPOS E PERFIS DE REDE .....                      | 34        |
| 5.2.5.1. VISITANTES .....                                 | 34        |
| 5.2.5.2. PROFESSORES.....                                 | 34        |
| 5.2.5.3. ALUNOS.....                                      | 35        |
| 5.2.6. KERBEROS .....                                     | 35        |
| 5.2.7. LDAP .....                                         | 35        |
| 5.2.8. ACCESS POINT .....                                 | 36        |
| 5.2.9. ILUSTRAÇÃO DA PROPOSTA.....                        | 36        |
| <b>6. CONCLUSÃO.....</b>                                  | <b>37</b> |
| <b>REFERÊNCIAS BIBLIOGRÁFICAS .....</b>                   | <b>38</b> |

## LISTA DE ILUSTRAÇÕES

|                                                           |    |
|-----------------------------------------------------------|----|
| Figura 1 – Exemplo de uma comunicação Ad Hoc .....        | 16 |
| Figura 2 – Repetição de um sinal Wireless .....           | 16 |
| Figura 3 – Equipamentos para a prática do WarDriving..... | 17 |
| Figura 4 – Símbolos do WarChalking.....                   | 18 |
| Figura 5 – Tela do AirSnort .....                         | 19 |
| Figura 6 – Tela do Kismet.....                            | 20 |
| Figura 7 – Tela do NetStumbler .....                      | 21 |
| Figura 8 – Firewall.....                                  | 21 |
| Figura 9 – Kerberos .....                                 | 25 |
| Figura 10 - Exemplo LDAP .....                            | 27 |
| Figura 11 - AP-3COM .....                                 | 27 |
| Figura 12 - AP-Mikrotik .....                             | 28 |
| Figura 13 - Pastas compartilhadas .....                   | 30 |
| Figura 14 - Acesso à unidade padrão .....                 | 31 |
| Figura 15 - Acesso às pastas compartilhadas .....         | 31 |
| Figura 16 - Realidade proposta.....                       | 36 |

## 1. INTRODUÇÃO

Com o crescente avanço tecnológico, o mundo está cada vez mais interligado à rede, resultando ao rápido acesso à informação, auxiliando dessa maneira os usuários no que diz respeito à troca de dados, comunicação, menor burocracia, entre outros fatores.

Com este progresso, surgem as redes sem fio, por proporcionar mobilidade, redução de custos na instalação e atender características exigidas pela empresa. Porém, a segurança desta tecnologia ainda demonstra ser crítica, pois, muitas redes são más configuradas e qualquer pessoa que estiver ao alcance do sinal poderá tentar quebrar as criptografias ou outros métodos de segurança existentes neles.

Ao estar no alcance desses sinais, qualquer indivíduo terá a possibilidade de utilizar técnicas capazes de capturar pacotes da rede e utilizar algoritmos para a quebra da chave de acesso. Existe também uma grande probabilidade de a rede estar aberta, assim sendo, o ingresso estará disponível sem nenhuma dificuldade.

## **2. OBJETIVOS**

### **2.1. OBJETIVO GERAL**

O objetivo deste trabalho é desenvolver um estudo sobre a vulnerabilidade da rede Wireless de uma instituição de ensino, apontando os pontos falhos e apresentando soluções para esta rede.

### **2.2. OBJETIVOS ESPECÍFICOS**

Os pontos abordados serão:

- Vulnerabilidade na autenticação
- Roubo de informações
- Limite de banda e controle de acesso
- Equipamentos utilizados
- Centralização das informações
- Solução dos pontos falhos

### **3. JUSTIFICATIVA**

Com a necessidade de mobilidade e comodidade, a instituição de ensino em estudo, adotou a utilização da rede wireless em suas dependências, e como todo processo trás aspectos bons e ruins, este não poderia ser diferente. Conjuntamente à aquisição deste tipo de ambiente, surgem também às várias formas de ataque, roubo de informações e modificação de documentos.

Devido ao fato de a rede desta instituição ser bastante requisitada por alunos e visitantes, é importante que haja uma renovação dos equipamentos, das políticas de segurança utilizadas e centralização das informações, a fim de manter seus usuários despreocupados quanto a uma possível invasão aos aparelhos em uso.

.

## 4. REFERENCIAL TEÓRICO

### 4.1. CRIPTOGRAFIAS

Atualmente, muitos dos métodos de segurança Wireless se baseiam em criptografias. Segundo Torres (2002), criptografia nada mais é que codificar dados em informações sem sentido algum, assim impossibilitando que pessoas consigam ter acesso a estas informações. A criptografia tem sido bastante útil no dia-a-dia, pois é utilizado em diversos serviços, como na proteção de dados, transmissão de arquivos online e em redes locais também, entre outros.

O método mais utilizado de criptografia é a da técnica de chave pública/privada. Nesta técnica de criptografia, uma fórmula matemática gera duas chaves, uma pública e outra secreta. Na chave pública, qualquer pessoa pode saber o que é utilizado para a criptografia dos dados, e na chave privada, somente o receptor conhece a chave que é utilizada para descriptografar esses dados, assim possibilitando a leitura da mesma. A idéia desta técnica é ter duas chaves distintas, impossibilitando a chave pública de descriptografar esses dados nem ter como decifrar a chave privada.

Agora é possível entender algumas das mais utilizadas Criptografias existentes nas redes Wireless.

#### 4.1.1. WEP (WIRED EQUIVALENT PRIVACY)

A citação abaixo determina de maneira simples o que seria a criptografia WEP para redes wireless.

Para Vasconcelos (2009), WEP é uma das mais antigas criptografias wireless. Nesta criptografia é possível trabalhar em 64 ou 128 bits, isso simplesmente muda o tamanho da senha a ser criada. Por ser bastante antiga, é a criptografia que tem grande número de notebooks e adaptadores sem fio compatíveis. Também por ser a mais antiga, é a mais vulnerável, pois as outras criptografias embaralham as senhas e o WEP não.

Ao realizar esta afirmação, Vasconcelos deixa à mostra que existem limitações nesta criptografia, por ser antiga e por suas senhas não serem embaralhadas, como as outras.

Mais a frente serão demonstrados alguns softwares capazes de quebrar esta criptografia.

#### 4.1.2. WPA (Wi-Fi Protected Access)

O WPA é uma criptografia Wireless, dizem ser o protocolo WEP melhorado, conhecido também por WPE2 ou TKIP (Temporal Key Integrity Protocol)<sup>1</sup>, esse protocolo surgiu com a necessidade de aumentar o nível de segurança das redes sem fio, em 2003, ajustando algumas vulnerabilidades existentes no WEP.

Com este protocolo, nota-se a melhora da criptografia em relação ao WEP, pois agora se utiliza de uma chave temporária (TKIP), possibilitando a criação de chaves por pacotes, outra vantagem é a melhoria na autenticação dos usuários, utilizando o 802.11x e EAP (Extensible Authentication Protocol), que através de um servidor faz a autenticação de cada usuário antes deste ter acesso à rede. No protocolo WPA, cada usuário tem sua própria senha, que deve ser digitada no momento da ativação WPA. Durante a sessão, esta chave é trocada periodicamente e automaticamente, assim dificultando ataques. Outra melhora em relação ao WEP é a chave de criptografia dinâmica, que diferentemente deste protocolo, não utiliza a mesma chave repetidamente nem exige que seja digitado manualmente.

#### 4.1.3. WPA2

Em 2004, a Wi-Fi Alliance teve a idéia de criar um certificado para redes Wireless mais confiáveis, e também para dar continuidade ao investimento realizado sobre o WPA.

Esta criptografia utiliza um protocolo denominado Advanced Encryption Standard (AES), método seguro e eficiente, porém, existem desvantagens em sua utilização, por exigir um processamento mais alto e prejudicar o desempenho dos equipamentos em uma rede sem muitos recursos físicos. Seu uso é adequado para quem necessita de uma proteção maior em sua rede.

Como dito anteriormente, o WPA2 utiliza-se do AES junto com o TKIP, com chave de 256 bits, sendo assim, um método bastante poderoso de criptografia.

---

<sup>1</sup> É um algoritmo de criptografia baseado em chaves que se alteram a cada novo envio de pacote. A sua principal característica é a freqüente mudança de chaves que garantem mais segurança. A senha é modificada automaticamente por padrão a cada 10.000 pacotes enviado e recebidos pela sua placa de rede.

## 4.2. VULNERABILIDADES

Junto com o avanço das tecnologias de redes Wireless vem também o crescente número de pessoas mal intencionadas querendo acessar as redes, com novas ferramentas surgindo todos os dias e o conhecimento se aprofundando ao longo do tempo, com isso se faz necessário ficarmos atentos às novas soluções de segurança a fim de diminuir as “brechas” deixadas por más configurações ou métodos ultrapassados nas redes Wireless. Para Roger (2006), no período de desenvolvimento das redes sem fio, um dos principais objetivos eram conectividade e acessibilidade de forma fácil, assim, a segurança da informação ficou em segundo plano. Logo se torna perceptível porque não é oferecida uma solução de segurança robusta.

### 4.2.1. VULNERABILIDADE DA CRIPTOGRAFIA WEP

Sendo bem antiga e não muito bem planejada, a criptografia WEP é bastante vulnerável. Por ter o tamanho limitado dos vetores de inicialização e ter chave estática. Se um hacker conseguir capturar pacotes por um determinado tempo, ele pode decifrar todos os pacotes em uma determinada rede. Veja um pequeno trecho retirado de uma reportagem postada no jornal eletrônico IDG NOW!, em abril de 2007:

(...) Matemáticos mostram desde 2001 falhas no protocolo WEP que permitem o cálculo do algoritmo após a detecção de certa quantidade de pacotes trocados. Brechas descobertas desde então derrubaram esta detecção, antes estimada em horas, para alguns minutos.

O novo estudo afirma que é necessário apenas três segundos para que uma chave de 104-bits de WEP seja interceptada para ser quebrada. Os dados necessários podem ser capturados em menos de um minuto, e o ataque exige menos poder de processamento que anteriores (...)

### 4.2.2. MÁ CONFIGURAÇÃO DOS ROTEADORES WIRELESS

Atualmente é comum encontrar uma rede doméstica sem nenhum tipo de proteção, pelo simples fato dos roteadores wireless virem de fábrica “pronto” para serem usados. Pela praticidade de instalação, os usuários esquecem de configurar uma senha de acesso às configurações do roteador e também algum tipo de proteção à rede sem fio, como pelo menos o filtro por MAC. As consequências da má configuração dos roteadores podem ser pesadas, como roubo de banda de internet, de dados sigilosos, propagação de vírus, e outros.

### 4.2.3. MAC SPOOFING

Antes mesmo de detalhar o funcionamento do MAC Address Spoofing, se faz necessário um breve comentário a respeito do MAC Address.

O MAC seria um endereço físico e único de cada interface de rede nos dispositivos, com combinações hexadecimais de 48 bits, das quais 24 bits são para identificação do fabricante e os 24 bits restantes para a identificação da interface. Esta combinação torna tal endereço físico único em todo mundo.

O endereço MAC pode ser considerado a “identidade” do dispositivo de rede, ao saber dessa informação, é possível se criar uma lista de acesso ou negação em uma rede wireless. Ao permitir tal MAC na rede, este dispositivo, ao alcance deste sinal, poderá conectar-se sem problemas. Sabendo que é possível a alteração do MAC via software, poderá ocorrer à prática do MAC Spoofing, que funciona utilizando-se das técnicas Eavesdrooping & Espionage<sup>2</sup>, possibilitando a captura de endereços MAC válidos para o acesso, alcançando uma invasão na rede.

## 4.3. SOLUÇÕES WIRELESS

### 4.3.1. AD HOC

Em redes cabeadas, para conectar dois dispositivos diretamente entre si, existe a possibilidade de utilizar cabos cross over para tal ação. Nas redes wireless esta idéia continua possível.

Ad Hoc, traduzido do latim ao pé da letra significa “Para Isto” ou “para esta finalidade”. Seu principal objetivo é conectar dois ou mais dispositivos wireless sem a necessidade de um ponto de acesso, ou seja, ligando-os entre si, sua velocidade de transmissão continua a mesma, porém, o alcance do sinal é menor, já que não possuem antenas com a mesma potência dos pontos de acesso.

---

<sup>2</sup> O Eavesdrooping & Espionage é basicamente uma técnica onde se captura e analisa todo o tráfego que passa na rede para utilizar os dados obtidos em possíveis ataques ou roubo de informações.



**Figura 1 – Exemplo de uma comunicação Ad Hoc**

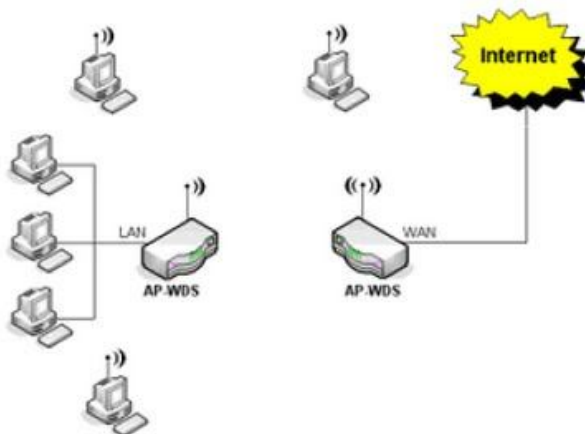
#### 4.3.2. REPETIÇÃO DE SINAL

Em alguns casos de redes, devido à distância, impossibilidade de cabeamento ou algum outro motivo, torna-se necessário à utilização de tráfego da rede por tecnologias wireless.

Ao utilizar certos dispositivos wireless a longa distância, pode haver perda de pacotes ou até mesmo a não comunicação entre os dispositivos, por causa da localização e/ou afastamento dos periféricos. Para solucionar este tipo de problema, existe um equipamento chamado Repetidor de Sinal Wireless, que capta todos os pacotes de um periférico e repassa para outro, assim evitando perda de pacotes e mantendo a comunicação entre eles.

Um grande problema da utilização desta tecnologia se dá pelo fato das interferências que podem ocorrer ao longo do caminho destes pacotes, pois, até mesmo como o nome sugere, ele repete o sinal e devido a frequência utilizada ser pública, pode haver algum tipo de “ruído”, que conseqüentemente o repetidor irá repassar para frente.

Na figura 2 segue um exemplo do funcionamento do repetidor de sinal wireless.



**Figura 2 – Repetição de um sinal Wireless**

#### 4.4. FERRAMENTAS

Existem diversas ferramentas capazes de mostrar informações das redes Wireless, como canal de funcionamento, frequência e criptografia utilizada. Essas informações podem ser úteis para consultoria, organização, e pra saber o nível de segurança alcançada, porém, também podem ser utilizadas com intenção de prejudicar o ambiente de rede.

Junto da expansão das redes wireless, estão crescendo também novas técnicas de ataque, que em alguns casos, o ataque pode ser bem sucedido em questão de segundos.

Roger ao comentar o crescimento das redes wireless fez a seguinte afirmação:

Ao mesmo tempo em que as redes wireless podem trazer praticidade, produtividade e até mesmo economia, elas representam um aumento de riscos aos processos de negócios, se não forem implementadas de modo adequado. Os perigos da utilização indiscriminada dessas redes são grandes. (Roger, 2006).

##### 4.4.1. WARDRIVING

É o ato de, na posse de um carro e equipamentos de rastreamento de sinais, como um notebook e um determinado tipo de antena conectado a ele, vasculhar redes abertas ou de criptografias falhas para uma possível invasão, roubo e/ou alteração de dados.

Um dos ataques mais comuns e comentados em redes wireless é o War Driving. Esse ataque tira proveito de uma característica fundamental: é difícil controlar e limitar o alcance de redes wireless. O atacante pode estar neste exato momento “passeando” no seu carro e com o laptop ligado “procurando” redes wireless vulneráveis. (Roger, 2006).

Na figura 3 é possível verificar o funcionamento do WarDriving, com todos os equipamentos necessários para vasculhar tais sinais.



**Figura 3 – Equipamentos para a prática do WarDriving**

#### 4.4.2. WARCHALKING

É feito escrevendo símbolos no chão, mostrando a existência de redes sem fio e suas configurações, indicando a posição da rede e facilitando o uso de conexões. Geralmente é feita em calçadas e a giz. Lembrando que esta prática só é possível com a utilização das técnicas do WarDriving.

| let's warchalk..! |                                  |
|-------------------|----------------------------------|
| KEY               | SYMBOL                           |
| OPEN<br>NODE      | ssid<br>bandwidth                |
| CLOSED<br>NODE    | ssid                             |
| WEP<br>NODE       | ssid access<br>contact bandwidth |

Figura 4 – Símbolos do WarChalking

Open Node: Este símbolo é utilizado para mostrar que a rede sem fio em questão está aberta, em outras palavras, seu SSID não está oculto, também informando a largura da banda da conexão.

Closed Node: Neste caso, o símbolo revela o oposto do Open Node, informando que a rede em questão tem seu SSID oculto.

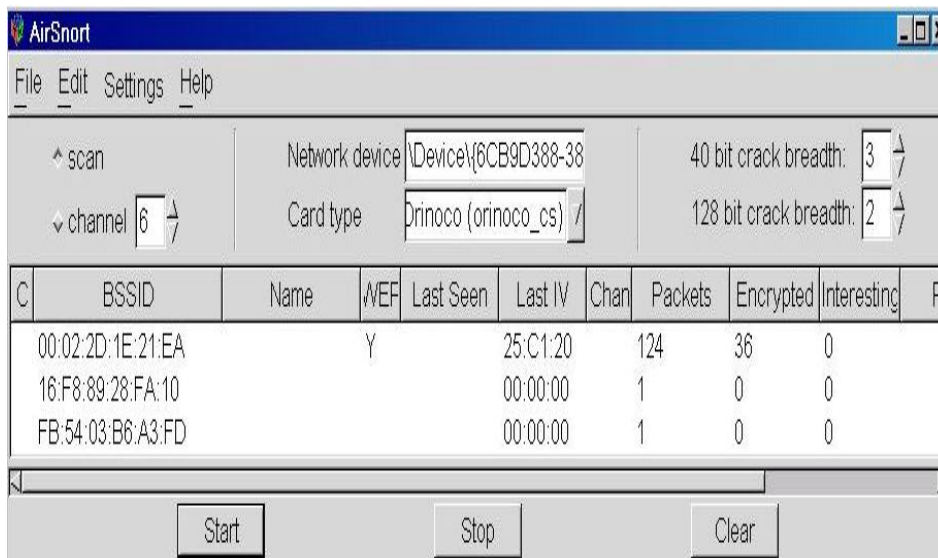
WEP Node: Já este símbolo informa que naquela área existe uma rede wireless, sendo protegida pela criptografia WEP.

#### 4.4.3. AIRSNORT

Este aplicativo funciona como um sniffer<sup>3</sup> de rede Wireless, ele tem o objetivo de quebrar chaves de criptografia WEP.

<sup>3</sup> Ferramentas utilizadas para capturar e opcionalmente analisar tráfego de rede.

O software monitora a rede e ao capturar uma quantidade suficiente de pacotes, ele se utiliza de algoritmos para a quebra dessa chave.



**Figura 5 – Tela do AirSnort**

#### 4.4.4. KISMET

Software desenvolvido para plataforma Linux: é uma ferramenta que pode ser usada para checagem da segurança da rede, verificar a existência de redes por perto e ter acesso a certas informações para uma configuração melhor da rede wireless, como o canal em que os sinais estão configurados.

Como é um programa feito para escanear redes sem fio, pode ser utilizada com más intenções, a fim de buscar redes desprotegidas ou descobrir redes com SSID ocultas para um possível ataque.

Ao ser ativado, o Kismet configura a placa wireless para o modo de monitoramento, não sendo possível usar tal placa para outros fins ao mesmo tempo, neste modo, o Kismet escuta todos os sinais que chegam a sua antena, assim funcionando como um scanner wireless.

Pelo fato do Kismet apenas escutar os sinais, não atrapalha tais redes ao seu redor e de forma quase indetectável.

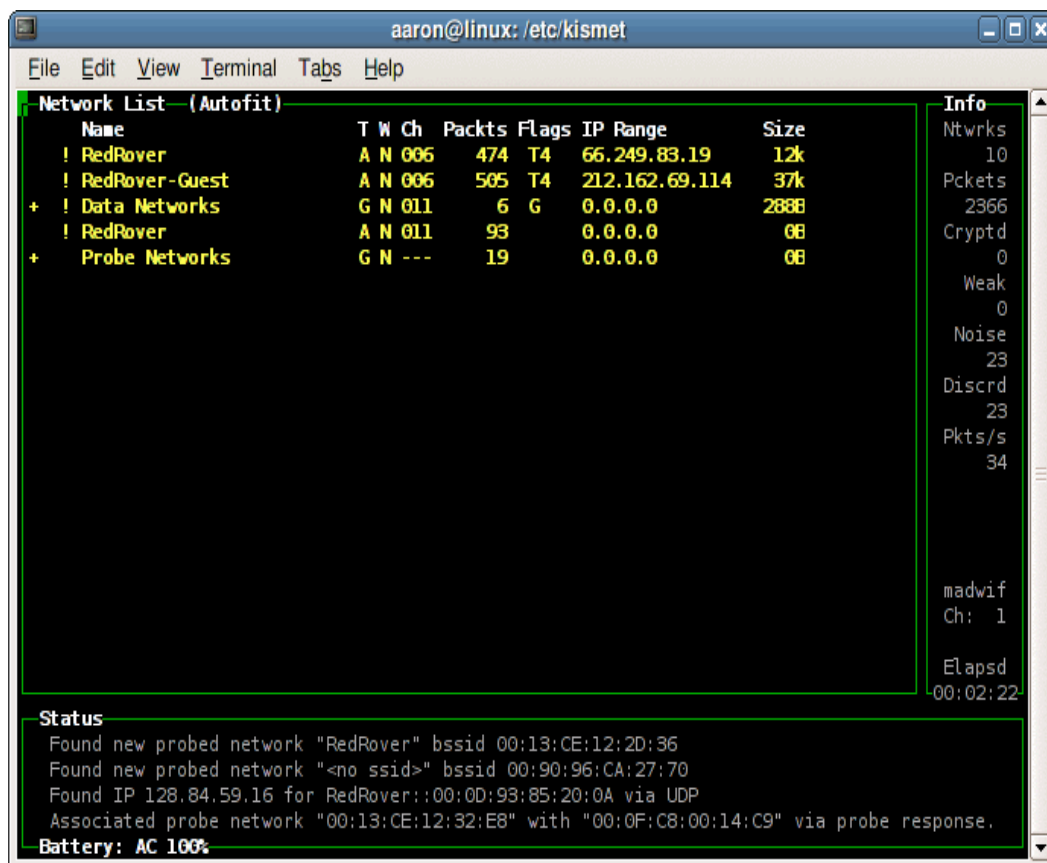


Figura 6 – Tela do Kismet

#### 4.4.5. NETSTUMBLER

Este software, assim como o Kismet, é uma ferramenta para verificar a segurança da rede wireless, feito para a plataforma Windows, é um dos mais eficazes na checagem da integridade e funcionamento da rede.

Ao encontrar novas redes, o NetStumbler insere o nome na lista, junto também de informações bem detalhadas em colunas separadas.

Este software é capaz de detectar pontos de acesso na área de cobertura da antena, mostrando a criptografia utilizada em cada rede, à intensidade do sinal e também tem a função de localizar setores defeituosos dentro de uma determinada rede, informando qual a origem do problema, que pode ser visualizada de forma clara em gráficos.

Com todas essas informações de uma rede, hackers de posse de outros programas, podem tentar quebrar criptografias, clonar MAC's, entre outros.

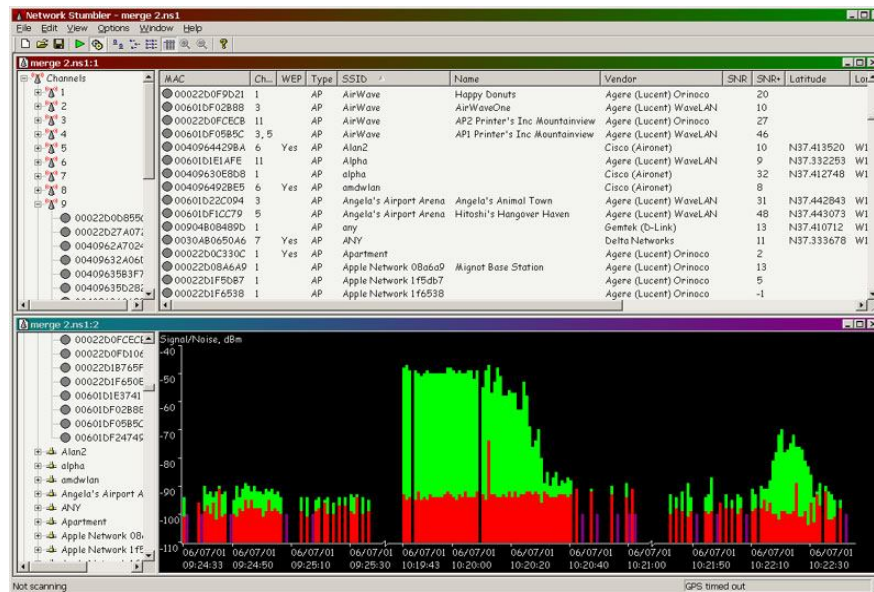


Figura 7 – Tela do NetStumbler

#### 4.5. SERVIDORES

Na área da computação, servidores são sistemas que fornecem serviços a uma rede, como no caso deste estudo, onde os servidores estarão rodando serviços de firewall, DHCP, e outros serviços.

##### 4.5.1. FIREWALL

Firewall (parede de fogo) tem sido cada vez mais importante na questão da segurança no mundo da computação. Com o avanço no uso de sistemas e informações, tal segurança necessita da aplicação de ferramentas e definições eficientes para a proteção do ambiente.



Figura 8 – Firewall

Este é o conjunto de recursos de programas e hardwares capazes de garantir a segurança de uma determinada rede. É um sistema que funciona com o objetivo de atuar como ponto único de defesa entre a rede privada e a pública, ou seja, a rede interna e a internet. Segundo Moraes (2008, p. 227), “O firewall controla todas as mensagens que passam por ele. Em geral um firewall é utilizado para interconectar uma rede segura (como a rede interna das empresas) com uma rede insegura como a Internet”.

Para Alecrim (2004), Existem dois tipos básicos de conceitos de firewalls: o que é baseado na filtragem de pacotes e o que é baseado em controle de aplicações. Ambos não devem ser comparados para se saber qual o melhor, uma vez que cada um trabalha para um determinado fim.

Conheceremos agora os dois tipos de conceitos de firewalls.

Filtragem de pacotes: É bastante utilizado em redes de pequeno ou médio porte. Este funciona com um montante de regras estabelecidas, onde são definidos quais endereços IPs e informações podem ter comunicação e quem poderá enviar ou receber essas informações. Certos serviços ou aplicações podem ser totalmente liberados ou bloqueados por padrão, devido aos seus possíveis riscos de segurança. O maior problema desse conceito é que certas regras aplicadas podem ter um nível elevado de complexidade, podendo não ser totalmente eficazes ou causar perda de desempenho na rede.

Este conceito trabalha nas camadas TCP/IP, determinando os pacotes de dados que poderão passar ou não. Estas são regras baseadas em informações do endereço IP remoto, endereço IP de destino e a porta TCP utilizada.

Quando o firewall está bem configurado, de acordo com os padrões e exigências da empresa, só serão permitidos que computadores autorizados pelas regras enviem ou recebam determinadas informações ou utilizem os devidos recursos liberados. O firewall também é capaz de analisar certas informações da conexão, determinar alterações suspeitas e tem o poder de verificar conteúdos dos pacotes, onde permite um melhor controle sobre o que pode ser acessível ou não.

Firewall de aplicação: Mais conhecido por Proxy, funciona como controle de aplicações HTTP, FTP, SMTP, entre outros. Este conceito não permite um contato direto entre o ambiente interno e a internet, assim sendo, tudo precisará passar pelo intermediário, que seria o firewall.

O firewall de aplicação é mais complexo que a filtragem de pacotes e também muito seguro, pois todas as aplicações precisam passar pelo Proxy, e sem ele, simplesmente não funcionarão.

Para Alecrim (2004), O firewall de aplicação permite um acompanhamento mais preciso do tráfego entre a rede e a internet (ou entre a rede e outra rede). É possível, inclusive, contar com recursos de log e ferramentas de auditoria. Tais características deixam claro que este tipo de firewall é voltado a redes de porte médio ou grande e que sua configuração exige certa experiência no assunto.

Alguns dos principais motivos do uso do Firewall são a de que ele ajuda a impedir que a rede seja acessada sem permissão, assim protegendo dados sigilosos. Outro motivo é que o firewall ajuda na prevenção de vírus, pois tem a capacidade de bloquear portas que podem ser utilizadas por certas aplicações, e também nas grandes redes corporativas, impedindo que usuários utilizem sistemas ou serviços que não são autorizados pela empresa.

O firewall vem demonstrando ser um recurso indispensável aos ambientes domésticos e corporativos, devido a sua grande importância e funções, autorizando quem deve ou não enviar ou receber tais pacotes, quem poderá acessar tais aplicativos ou páginas da internet, também evitando acesso à rede por pessoas sem permissão, protegendo dados e informações preciosas e/ou sigilosas, ajuda no combate aos vírus nos computadores, preservando a integridade e bom funcionamento da rede.

#### 4.5.2. DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL)

O DHCP ou Protocolo de Configuração Dinâmica de Endereços de Rede é um protocolo que permite que os computadores recebam suas configurações de rede diretas de um servidor. Ao ser configurado e em funcionamento, o DHCP atribui endereços IP dinamicamente, sem a necessidade de configuração nas estações de trabalho.

Para BADDINI: “Não só o endereço IP de elementos de rede são entregues e gerenciados pelo servidor DHCP, mas também todas as configurações de rede necessárias para um funcionamento otimizado e estável da rede”. Essas configurações seriam Endereço IP, máscara de sub-rede, Servidor DNS, entre outros.

Uma boa funcionalidade do DHCP é a criação de Escopos de Rede, pelo qual o administrador define que faixa de endereços IPs será disponibilizada de forma automática na rede, podendo assim deixar uma faixa de IP reservados para servidores, roteadores e outros

serviços. Uma outra configuração interessante é a reserva de IP, onde pode se atribuir um endereço IP para um determinado endereço MAC.

Este serviço de rede, como qualquer outro centralizado é uma forma de facilitar o gerenciamento e configurações para o administrador, pois todas as suas alterações seriam efetuadas diretamente no servidor, sem necessidade de alterações nos computadores, podendo também trabalhar com diversos escopos, podendo facilitar a manutenção dos grupos de rede.

#### 4.5.3. KERBEROS

Antes de explicar o funcionamento e importância do Kerberos, é necessário antes fazer uma explanação dos motivos de sua existência, como na descrição abaixo:

A internet é um local inseguro, e esta insegurança está vinculada diretamente aos protocolos que não oferecem níveis de segurança adequados. Esses protocolos possibilitam a pessoas mal intencionadas executarem programas sniffers (farejadores) para capturarem pacotes. E, em um desses pacotes capturados, podem estar as senhas da rede.

Isto só acontece porque as senhas transferidas entre o servidor e o cliente descriptografadas (Clean Text), e os programas servidores confiam na honestidade do cliente(...). TRIGO (2007, p. 88).

De acordo com o que foi visto, agora é possível identificar os motivos pelos quais o MIT<sup>4</sup> desenvolveu o Kerberos.

O Kerberos é um protocolo de autenticação, que permite a comunicação segura e individual em uma rede insegura. Graças a sua criptografia forte o cliente precisa provar sua identidade ao servidor e vice-versa. Depois de provar sua identidade utilizando o protocolo Kerberos, o mesmo pode criptografar os dados, garantindo a integridade e a privacidade dos arquivos durante a conexão.

O Kerberos utiliza-se de dois tipos de chaves como método de identificação. São elas:

- Chave secreta: este tipo de chave é utilizado para efetuar o logon no ambiente de rede, neste caso, o usuário e o kerberos devem conhecer a chave. Antes desta autenticação, usuário e chave de sessão devem existir no banco de dados do Kerberos.

---

<sup>4</sup> Massachusetts Institute of Technology (Instituto Tecnológico de Massachusetts)

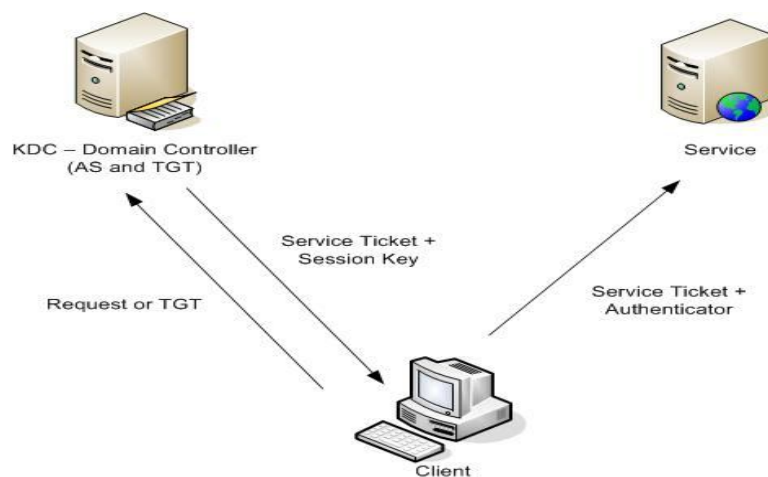
- Chave de Sessão: este tipo de chave é criado depois que o usuário faz a autenticação no ambiente, tendo por finalidade autenticar o canal, garantindo que os dados transferidos sejam mesmo de tal usuário.

Além dos dois tipos de chaves para identificação do usuário junto ao Kerberos, existem também dois tipos de credenciais, que são:

- Ticket: é um certificado temporário distribuído pelo Kerberos. (TRIGO, 2007, p. 91). Nesta chave, também é criptografado a chave secreta do usuário, a fim de confirmar se o usuário é ele mesmo.
- TGT<sup>5</sup>: (...) certificado que permite ao usuário se identificar na rede e receber ticket sob demanda, sempre que quiser estabelecer uma conexão com outro usuário ou com um serviço – ou seja, é um “ingresso que valida ingressos”. (TRIGO, 2007, p 91).

O funcionamento do Kerberos se dá nos seguintes passos:

Na primeira etapa, quando o cliente tenta se autenticar ao servidor, envia uma solicitação de autenticação ao KDC (Key Distribution Center – Centro de Distribuição de Chaves). Na segunda etapa, o KDC ao verificar se a conta realmente existe no banco de dados, cria e envia uma TGT criptografada usando a senha do cliente. A terceira e última etapa, a TGT é descriptografada pelo cliente utilizando sua senha, assim tendo autorização para utilizar o serviço solicitado.



**Figura 9 – Kerberos**

---

<sup>5</sup> Ticket-Granting Ticket

#### 4.5.4. LDAP (LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL)

Para melhor entendimento do LDAP, é preciso uma compreensão do conceito de diretórios, que pode ser definido das seguintes formas:

“Tabela com identificadores e referências aos itens de dados correspondentes”  
(Dicionário do Aurélio)

Ou então:

“Índice usado por um programa de controle para localizar um ou mais blocos de dados separados, de um conjunto de dados armazenados em um meio de acesso direto”. (Dicionário do Aurélio)

Para TRIGO, o LDAP, ou Protocolo Leve de Acesso a Diretórios, é basicamente um organizador controlando a comunicação entre os serviços de diretórios e de seus clientes através de uma série de regras.

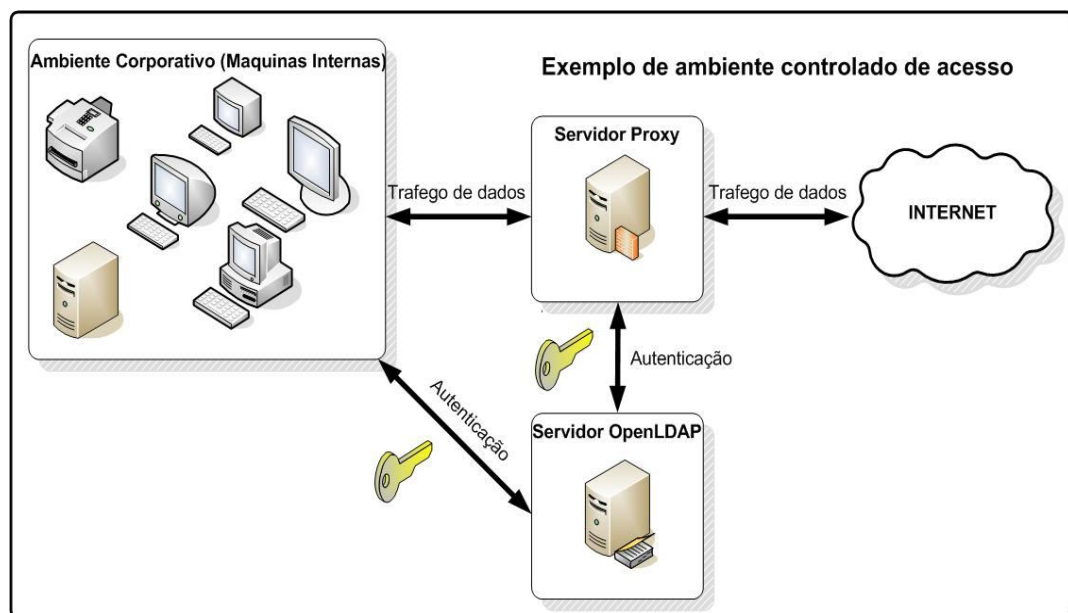
MORIMOTO afirma que uma das principais vantagens do LDAP se dá pelo fato da facilidade de localizar informações e arquivos, exemplificando que é possível localizar dados como, telefone ou endereço de um funcionário apenas fazendo uma busca por seu sobrenome.

O LDAP pode ser utilizado em serviços como, Samba, apache, E-mail, Proxy entre outros. Tudo isso com a idéia de que a base de dados dos usuários estará armazenada nele.

Por ser um padrão aberto, capaz de facilitar o compartilhamento e gerenciamento de um grande volume de informações, o protocolo LDAP tem sido muito importante.

Existe uma série de aplicativos que podem ser suportados por este protocolo, podendo até trabalhar com a mesma base de dados, facilitando a vida dos administradores de rede, que, por exemplo, o usuário ao alterar sua senha, automaticamente todas as outras aplicações irão utilizar esta nova senha, sem a necessidade de alterar em todos os aplicativos.

Por motivos de segurança, o LDAP deve vir seguido de uma política forte de senhas, pois, ao descobrir uma senha, um hacker teria acesso a todas estas aplicações.



**Figura 10 - Exemplo LDAP**

#### 4.6. EQUIPAMENTOS

Em toda empresa que preza pela qualidade e bom funcionamento de seus serviços, admitem a idéia de renovação constante de certos equipamentos, principalmente os de informática, que sempre vem sofrendo atualizações e melhorias quanto à qualidade de seus produtos.

Devido à proposta de mudança em algumas políticas adotadas na instituição, é sugerida a aquisição de alguns equipamentos para um bom padrão do funcionamento da estrutura do ambiente.

##### 4.6.1. ACCESS POINTS

##### 4.6.1.1. ACCESS POINT 3COM



**Figura 11 - AP-3COM**

Dentre os equipamentos esta é uma solução Wireless de ótimo custo benefício para empresas de todos os portes. O equipamento possui radio dual com recursos completos e funciona com diversos padrões de forma simultânea. Funciona com velocidade de até 108 Mbps, assim melhorando o tráfego entre o dispositivo wireless e a rede. Cada equipamento deste modelo tem suporte para até 128 usuários em sua rede local, assim possibilitando o crescimento da rede em questão.

O valor médio para este produto, em Novembro/2010 era em torno de R\$ 1.180,00. Isto por causa da capacidade técnica, eficácia e qualidade que é oferecida a empresa.

#### 4.6.1.2. ROUTERBOARD

A RouterBoard é um poderoso Access Point/Roteador.

Este produto possui 128MB DDR de RAM e 64MB de capacidade de armazenamento, além da entrada de cartões de memória MICROSD, aumentando sua capacidade de armazenamento de dados em cache.

Uma das principais características desse equipamento é seu processador de alto desempenho Atheros AR7161 de 680MHz, permitindo maior desempenho em análise e processamento de pacotes por segundo, obtendo taxas maiores de tráfego na rede.

Esta RouterBoard possui 3 portas Fast Ethernet 10/100 Mbit além de três slots para cartões MiniPCI, garantindo uma maior performance em aplicações de distribuição de sinal.

Seu sistema operacional, voltado para aplicações de rede, possui recursos como roteamento, firewall, gestão de controle de acesso, controle de banda, balanceamento de link, servidor dhcp, DNS, além de outros recursos.

Este equipamento é muito bem utilizado para aplicações de distribuição de sinal WI-FI de alto desempenho em empresas, provedores de internet, prefeituras, links de tráfego de imagens e voz sobre IP.



**Figura 12 - AP-Mikrotik**

Suas principais características podem ser resumidas abaixo:

- Processador de alto desempenho Atheros 680MHz
- Memória de 128MB DDR
- Três portas Fast Ethernet 10/100Mbps/s
- Roteamento e firewall
- Gestão de controle de acesso, controle de banda
- DNS e DHCP
- Balanceamento de link.
- Entrada para cartão MICROSD
- 64MB de memória para cache.
- Sistema operacional voltado para aplicações de rede
- Link de tráfego de imagem
- Link de tráfego de voz sobre IP
- Altas taxas de tráfego na rede

Por sua importância para muitas aplicações e recursos em uma rede, seu valor, de certa forma é bastante acessível, em Novembro/2010 estava na faixa de R\$ 500,00.

## 5. ESTUDO DE CASO

Em uma instituição de ensino, tendo em vista a qualidade de aprendizagem, conforto e comodidade aos seus professores, alunos e visitantes, foi disponibilizada Internet Wireless (sem fio) em vários pontos de seu amplo espaço físico, com a intenção de interligá-los ao mundo com o uso dessa tecnologia.

Ao chegar a um destes pontos de acesso à rede wireless, é possível notar a falta de tecnologias e ferramentas de segurança para que, além do conforto e comodidade proposta pela instituição, obtenha também confiança de que poderá conectar-se sem ter problemas futuros, como roubo de dados e senhas, e várias outras possibilidades.

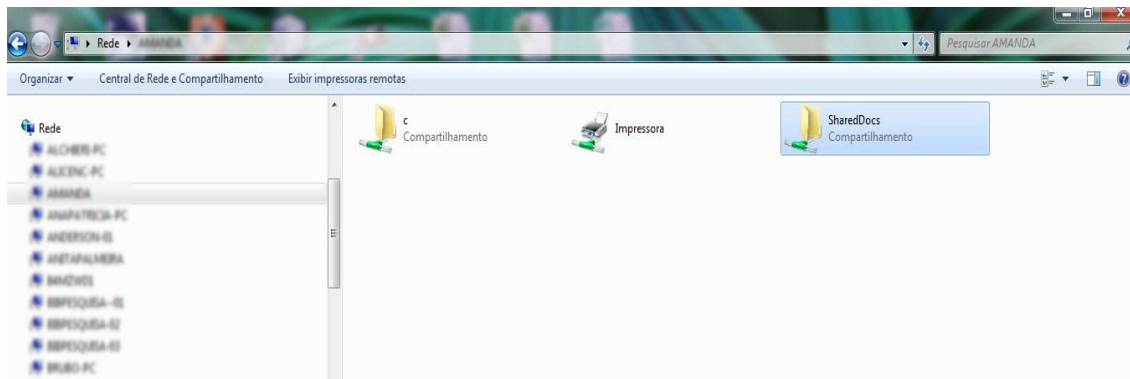
A idéia de segurança mais indicada para este caso seria utilizar servidores, aplicativos e equipamentos capazes de rodar firewall, criar perfis e regras de acesso, centralizar o gerenciamento das configurações e também, controlar o tráfego e páginas acessadas por seus usuários.

Nos tópicos abaixo, ficará explícito como é o funcionamento atual, uma explicação a respeito dos servidores, equipamentos e configurações a realizar e uma proposta de como poderia ser o funcionamento destas idéias de segurança.

### 5.1. REALIDADE ATUAL

Ao acessar e vasculhar a rede em estudo, é perceptível a facilidade de roubo de informações no ambiente.

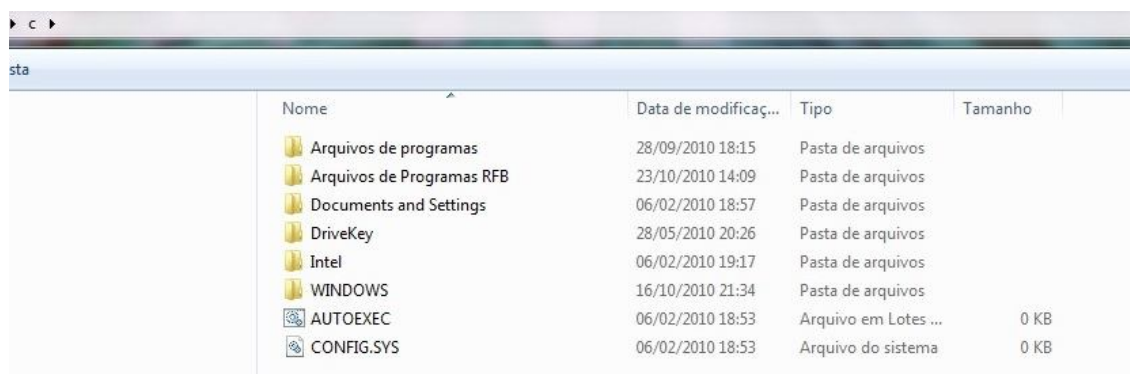
Nas figuras 13, 14 e 15 estarão comprovados alguns exemplos desta facilidade.



**Figura 13 - Pastas compartilhadas**

Na figura 13, a lista da esquerda mostra os computadores da rede que puderam ser identificados, ao centro, está mostrando as pastas e impressoras compartilhadas em um computador na rede em estudo.

Nas figuras 14 e 15, é possível mostrar que o computador acessado em questão está liberando suas pastas compartilhadas para todos os usuários, tornando possível o acesso à unidade padrão do computador e à pasta de compartilhamento do S.O. (Sistema Operacional), tendo acesso à pasta de fotos do computador.

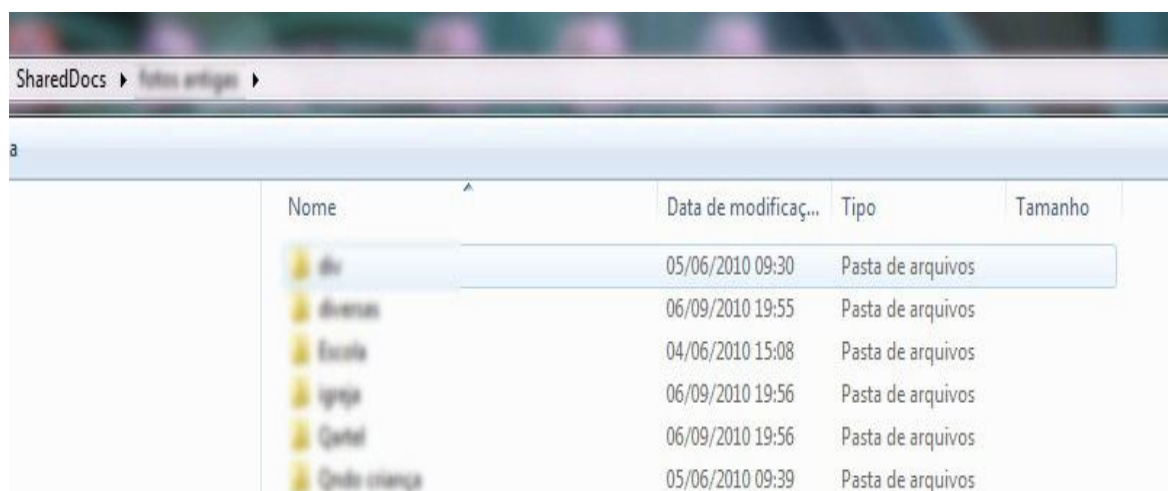


| Nome                      | Data de modificaç... | Tipo                 | Tamanho |
|---------------------------|----------------------|----------------------|---------|
| Arquivos de programas     | 28/09/2010 18:15     | Pasta de arquivos    |         |
| Arquivos de Programas RFB | 23/10/2010 14:09     | Pasta de arquivos    |         |
| Documents and Settings    | 06/02/2010 18:57     | Pasta de arquivos    |         |
| DriveKey                  | 28/05/2010 20:26     | Pasta de arquivos    |         |
| Intel                     | 06/02/2010 19:17     | Pasta de arquivos    |         |
| WINDOWS                   | 16/10/2010 21:34     | Pasta de arquivos    |         |
| AUTOEXEC                  | 06/02/2010 18:53     | Arquivo em Lotes ... | 0 KB    |
| CONFIG.SYS                | 06/02/2010 18:53     | Arquivo do sistema   | 0 KB    |

**Figura 14 - Acesso à unidade padrão**

Nesta figura, está listando algumas pastas padrões do S.O., como a pasta “arquivos de programas”, a pasta “documents and Settings”, onde ficam armazenados os programas instalados e arquivos pessoais do usuário.

Já na figura 15, será possível perceber que se trata de uma pasta de fotos pessoais do usuário, assim evidenciando uma invasão de privacidade, que a instituição faz tornar possível.



| Nome          | Data de modificaç... | Tipo              | Tamanho |
|---------------|----------------------|-------------------|---------|
| div           | 05/06/2010 09:30     | Pasta de arquivos |         |
| diversas      | 06/09/2010 19:55     | Pasta de arquivos |         |
| Escola        | 04/06/2010 15:08     | Pasta de arquivos |         |
| Igreja        | 06/09/2010 19:56     | Pasta de arquivos |         |
| Gente         | 06/09/2010 19:56     | Pasta de arquivos |         |
| Quêdo criança | 05/06/2010 09:39     | Pasta de arquivos |         |

**Figura 15 - Acesso às pastas compartilhadas**

Estes foram alguns exemplos de como roubar dados em uma rede insegura, somente através de um rápido “vasculhamento” na rede, sem nenhum tipo de aplicativo específico.

Também surge a necessidade da verificação do servidor proxy, que além de limitar o acesso às páginas da internet, também deve funcionar como servidor cache, o que não está ocorrendo em nenhum dos dois casos na empresa em estudo.

Além de todos esses problemas encontrados, nota-se que não existe um limite de banda para os usuários da rede, tornando a navegação um pouco precária, pelo fato de algumas pessoas poderem “roubar” boa parte dela para downloads em geral.

Em cima destas falhas mostradas foi feito uma análise, e nas seções seguintes serão mostradas algumas sugestões para a melhoria de segurança e acesso, assim causando um melhor desempenho da rede.

## 5.2. REALIDADE PROPOSTA

A proposta sugerida à instituição poderia ser bem sucedida com a aquisição de alguns equipamentos, como servidores LDAP e Kerberos, roteador Mikrotik (para gerenciamento das configurações), Access Points 3COM, a reconfiguração do servidor Proxy da empresa, criação de escopos no DHCP, e outras configurações.

### 5.2.1. ROUTERBOARD MIKROTIK

O uso da RouterBoard Mikrotik será de fundamental importância, pois esta RouterBoard irá trabalhar como servidor DHCP, criando escopos entre os grupos dos Professores, Alunos e Visitantes, também irá trabalhar no gerenciamento da banda para esses grupos, funcionando no bloqueio de portas da rede.

### 5.2.2. DHCP

Para garantir a segurança da rede wireless, serão configurados escopos no DHCP da RouterBoard, que irão distribuir IP's aos dispositivos dos usuários, tendo um escopo diferente para os Grupos Professores, Alunos e Visitantes, onde nos dois primeiros grupos serão associados o IP ao escopo pelo MAC Address dos dispositivos, sendo que cada escopo irá funcionar em redes distintas. Já todos aqueles dispositivos que não tiverem seu MAC cadastrado no DHCP, será automaticamente redirecionado para um terceiro escopo, destinado

aos Visitantes. Abaixo será explicado como poderá ser o funcionamento da divisão das redes Wireless, adotando a máscara 255.255.255.0:

Professores: 10.10.1.x

Alunos: 10.10.2.x

Visitantes: 10.10.3.x

Com estas configurações, cada grupo funcionará em uma rede diferente, impossibilitando a comunicação entre redes distintas.

Ao usar essas faixas de IP, melhora na organização do ambiente, assim, criando uma rede para cada grupo de usuários.

### 5.2.3. PROXY

No uso de servidor Proxy para professores e alunos, pode utilizar o Proxy com autenticação, utilizando o protocolo Kerberos, para uma melhor segurança no envio e recepção de pacotes. Já para o grupo Visitantes, é sugerida a configuração de um Proxy transparente, pois os visitantes do local não terão que cadastrar o MAC do dispositivo junto à gerência de informática, assim tendo certos bloqueios em relação aos demais grupos.

No caso do bloqueio de páginas, os grupos Alunos e Visitantes, irão ter permissões de acesso iguais, sem permissão a sites de relacionamento e outras páginas que não são de importância acadêmica. Já o grupo Professores não terá nenhum bloqueio, pela sua importância de seus acessos a qualquer tipo de página.

Será preciso uma configuração de cache neste serviço, pois ao avaliar este quesito, nota-se a ausência da mesma.

A diferença entre os grupos Alunos e Visitantes se dará pelo limite de banda fornecido a cada grupo, onde os alunos irão desfrutar de um limite superior em relação aos visitantes (que será configurado para a faixa de IP de cada escopo), pelo fato do grupo ter mais usuários que o grupo dos visitantes. No caso do grupo Professores, o limite será maior ainda em relação aos demais, por se tornar necessário que eles tenham certas “regalias”, por causa de sua importância acadêmica.

#### 5.2.4. BLOQUEIO DE COMPARTILHAMENTO

Um dos maiores equívocos encontrados no atual estudo foi a liberação de compartilhamento de arquivos, demonstrado no tópico da Realidade Atual, onde com uma rápida vasculhada na rede pode-se encontrar diversos dispositivos compartilhando recursos, como por exemplo impressoras e principalmente arquivos.

Para solucionar este problema, pode-se configurar no firewall o bloqueio de algumas portas padrões de compartilhamento de recursos, como as portas 137 a 139 e também a porta 445, assim desabilitando a busca de compartilhamentos na rede e acesso a arquivos e impressoras.

#### 5.2.5. GRUPOS E PERFIS DE REDE

Para melhor organização e praticidade quanto às permissões a recursos que a rede pode oferecer e páginas que podem acessar, torna-se necessário a implementação de grupos e perfis de rede, onde cada usuário dos grupos Professores e Alunos terão seu próprio login, e cada login terá suas respectivas regras de acesso. Já para o grupo Visitantes, é sugerido que o Proxy seja transparente, pela impossibilidade do controle desse tipo de usuário e pela grande demanda de visitantes à instituição de ensino estudada. Assim não terá a necessidade de cadastro de dispositivo junto à instituição.

##### 5.2.5.1. VISITANTES

Os visitantes, por serem pessoas que não estarão na instituição com tanta frequência e para não prejudicar a rede utilizando grande parte da banda, terão restrições maiores se comparados aos outros grupos, bem como, limite de tráfego, restrições a certos aplicativos, como Messengers em geral.

##### 5.2.5.2. PROFESSORES

Os professores terão certas “regalias” que os diferem dos outros grupos. Estes terão limites de tráfego maior que os demais, pela importância do seu trabalho junto à instituição de ensino e desfrutará de total acesso às páginas da Internet.

Cada usuário deste grupo poderá solicitar junto à gerência de informática a criação de uma pasta na rede para arquivamento de documentos importantes nos servidores da empresa e terão permissão para acesso aos Messengers em geral.

#### 5.2.5.3. ALUNOS

O grupo dos alunos será um meio termo entre os outros dois grupos, ou seja, não terão acesso total como os professores e nem o limite de banda tão restrito quanto os visitantes. Eles poderão usufruir de certas páginas da internet, terão a capacidade de realizar todas suas pesquisas acadêmicas sem nenhum tipo de problema, porém, terão restrições às páginas de relacionamento. O limite da banda será um pouco menor que a dos professores, assim acabando com certos problemas de banda que ocorrem no local. Cada usuário deste grupo poderá solicitar a criação de seu webmail, terá acesso ao sistema de notas e histórico, também obtendo acesso ao moodle da instituição de ensino.

#### 5.2.6. KERBEROS

Para maior segurança e integridade da rede, é sugerido o Kerberos para funcionar como servidor de autenticação, através de uma série de procedimentos, o usuário tem que provar ao servidor que é ele mesmo que está de posse do dispositivo e vice versa, pois todos pensam que o problema só está do lado de fora, o que em alguns casos não é verdade.

#### 5.2.7. LDAP

No LDAP estarão armazenadas as informações dos usuários da rede, pela sua agilidade na busca de informações no diretório, tornou-se importante a sugestão desta tecnologia a este ambiente.

Ao enviar uma solicitação de logon na rede, o servidor Kerberos irá verificar os dados do usuário no diretório LDAP, verificando se aquelas informações estão corretas e o Kerberos continuando com o procedimento de logon do usuário.

Com esta idéia do uso do LDAP, podem-se integrar vários sistemas utilizados na instituição usando a mesma base de dados. Assim, possibilitando ao usuário ter apenas um login e senha para ter acesso a vários recursos que a instituição pode oferecer.

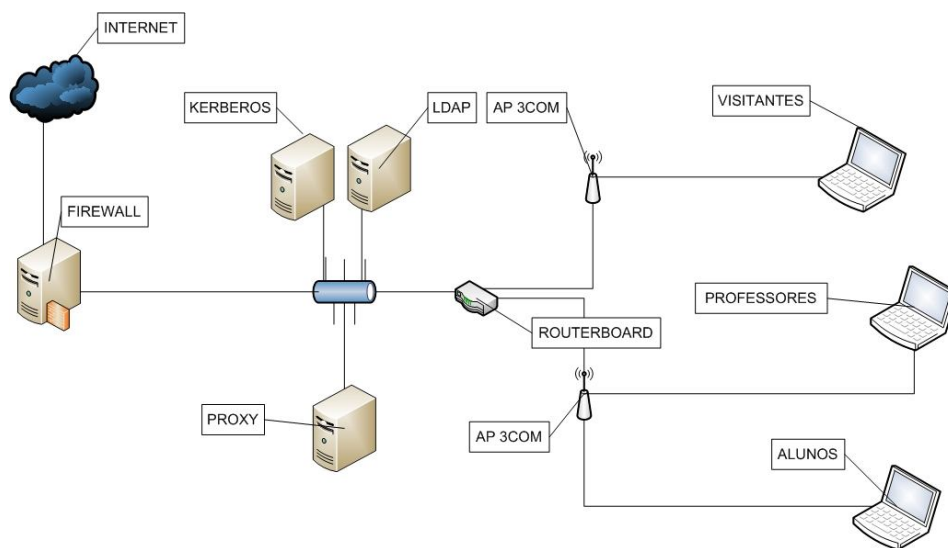
### 5.2.8. ACCESS POINT

Ao sugerir à aquisição do Access point, foi levada em consideração a qualidade que a rede pode obter com esta tecnologia, pelo fato do sinal deste equipamento ter um grande alcance, impossibilitará a queda de conexão nos dispositivos.

Partindo da suposição que os visitantes irão se concentrar em alguns lugares, a idéia é ter Access Points exclusivos a este grupo em alguns pontos da instituição, já nos grupos Professores e Alunos, a idéia é fornecer Access Points exclusivos em toda estrutura da instituição.

### 5.2.9. ILUSTRAÇÃO DA PROPOSTA

A proposta deste projeto, de acordo com a análise da pesquisa efetuada na instituição, poderá ser exemplificada na figura 16.



**Figura 16 - Realidade proposta**

## 6. CONCLUSÃO

Este projeto envolveu um estudo sobre diversas ferramentas, técnicas, criptografias e tecnologias utilizadas em redes wireless, a fim de mostrar a importância de seus recursos, assim, fazendo uma abordagem à rede wireless da instituição de ensino em estudo, mostrando suas vulnerabilidades (falhas), equívocos administrativos e alguns outros pontos que podem ser melhorados.

Como a rede wireless em estudo tem um nível muito alto de acesso, tornou-se interessante fazer um estudo sobre a mesma, identificando falhas, como demonstrado nos capítulos anteriores, sugerindo algumas correções e uma mudança na política da empresa.

Ao estudar as criptografias de modo geral, nota-se seu grau de importância, não só nas redes wireless, mas em qualquer meio de transmissão de dados existentes, o que não existe na rede wireless em estudo.

Algumas vulnerabilidades foram encontradas, bem como o acesso a alguns recursos de rede, como o compartilhamento de arquivos e impressoras. Também foram identificadas algumas outras falhas, como a ausência de um servidor proxy ou a má configuração da mesma.

Com a inexistência do limite de banda nesta rede, é possível que um usuário "roube" boa parte da banda de internet para downloads em geral. Notou-se que não existe uma política de grupo nem de acesso a esta rede, possibilitando o acesso a qualquer página da internet por parte de qualquer pessoa que estiver ao alcance deste sinal, o que não é uma grande vantagem para a empresa.

Com todas essas informações dadas, foi possível chegar a algumas soluções, que de acordo com certo estudo em cima dessas falhas, puderam ser sugeridas na realidade proposta deste projeto.

## REFERÊNCIAS BIBLIOGRÁFICAS

- ABBAS, Ali Abou. **Squid autenticando em OpenLDAP + Debian 5.0**. Disponível em: <<http://discipulosdopinguim.com.br/novidades/squid-autenticando-em-openldap-debian-5-0-lenny>>. Acesso em 19 de Nov. de 2010.
- AIRSNORT. **AirSnort**. Disponível em: <<http://airsnort.shmoo.com/>>. Acesso em 28 de Jul. de 2010.
- ALECRIM, Emerson. **Firewall: Conceitos e Tipos**. Disponível em: <<http://www.infowester.com/firewall.php>>. Acesso em 7 de ago. de 2010.
- AREPLAWU. **Warchalking**. Disponível em: <<http://cara-hacking-tool.blogspot.com/>>. Acesso em 13 de Nov. de 2010.
- AUGUSTO, Danilo. **Entenda de uma vez por todas o que é o endereço MAC**. Disponível em: <<http://www.iotecnologia.com.br/entenda-de-uma-vez-por-todas-o-que-o-endereo-mac/>>. Acesso em 25 de set. de 2010.
- BADDINI, Francisco. **Windows Server 2003 em português**. 7 ed. São Paulo: Érica, 2008.
- CARDIA, ANDRÉ. **Firewall**. Disponível em: <<http://andrecardia.pro.br/>>. Acesso em 12 de Nov. de 2010.
- DAMON. **Wardriving**. Disponível em: <<http://dcortesi.com/>>. Acesso em 11 de Set. 2010.
- DICIONÁRIO DO AURÉLIO. **Significado de Diretório**. Disponível em: <<http://www.dicionariodoaurelio.com/Diretorio>>. Acesso em 21 de ago. de 2010.
- GANEM, Igor de Oliveira. **Seguranças e criptografias nos Access points**. Disponível em: <<http://www.vivaolinux.com.br/artigo/Seguranca-em-redes-wireless?pagina=2>>. Acesso em 09 de mai. 2010.
- INACIO, Alexandre. **Segurança de rede wireless**. Disponível em: <<http://www.forumpcs.com.br/review.php?r=266078>>. Acesso em 02 de mai. 2010.

- INVICEBLOG. **NetStumbler**. Disponível em:  
<<http://invincible.wordpress.com/?s=netstumbler>>. Acesso em 28 de Jul. de 2010.
- LIMA, Marco Aurelio de. **WEP**. Disponível em:  
<[http://www.malima.com.br/blog/blog\\_commento.asp?blog\\_id=29](http://www.malima.com.br/blog/blog_commento.asp?blog_id=29)>. Acesso em 02 de mai. 2010.
- MATTHEWS, Daren. **Kerberos**. Disponível em: <<http://mccltd.net/>>. Acesso em 19 de Nov. de 2010.
- MENEZES, Ricardo. **Warchalking**. Disponível em:  
<<http://www.vivasemfio.com/blog/category/warchalking/>>. Acesso em 02 de mai. 2010.
- MICROSOFT. **Planejar proteção de segurança**. Disponível em:  
<<http://technet.microsoft.com/pt-br/library/cc262849.aspx>>. acesso em 15 de Nov. de 2010.
- MONTEIRO, Amadeu Pires. **MIT**. Disponível em:  
<<http://www.dicionarioinformal.com.br/definicao.php?palavra=mit&id=2370>>. Acesso em 7 de ago. de 2010.
- MORAES, Alexandre Fernandes. **Redes de computadores – fundamentos**. 6. ed. São Paulo: Érica, 2008.
- MORIMOTO, Carlos E. **LDAP**. Disponível em:  
<<http://www.guiadohardware.net/termos/ldap>>. Acesso em 06 de nov. de 2010.
- NOVA NETWORK. **RouterBoard Mikrotik**. Disponível em:  
<<http://www.novanetwork.com.br/produtos/det/rb433ah/8/mikrotik/placas-routerboard/routerboard-mikrotik/routerboard-mikrotik-rb433ah.php>>. Acesso em 14 de ago. de 2010.
- OTÁVIO, Luiz. **Termos mais comuns em configurações wireless**. Disponível em:  
<<http://blogger.todospacoonline.com/2009/07/termos-mais-comuns-em-configuracoes.html>>. Acesso em 19 de Nov. de 2010.
- POWER COMP. **Access Point 3COM**. Disponível em:  
<[http://www.pccomputadores.com.br/comprar/access\\_point\\_3com\\_3crwe876075\\_rj-45\\_ieee\\_802.11a-b-g\\_108mbps.html](http://www.pccomputadores.com.br/comprar/access_point_3com_3crwe876075_rj-45_ieee_802.11a-b-g_108mbps.html)>. Acesso em 14 de ago. de 2010.

- ROGER, Denny. **Teste de invasão em redes wireless**. Disponível em: <<http://blog.dennyroger.com.br/2006/04/06/teste-de-invasao-em-redes-wireless/>>. Acesso em 10 de abr. 2010.
- \_\_\_\_\_. **Técnicas de ataques em redes Wireless**. Disponível em: <<http://www.forum-seguranca.com/artigo/single-artigo-view/article/tecnicas-de-ataques-em-redes-wireless/7.html>>. Acesso em 24 de abr. 2010.
- SAYER, Peter. **Ataques e ameaças**. Disponível em: <<http://idgnow.uol.com.br/seguranca/2007/04/04/idgnoticia.2007-04-04.5273476708/>>. Acesso em 17 de abr. 2010.
- TANEMBAUM, Andrew S. **Computer networks**. 4. ed. Editora: Prentice-Hall, 2003.
- TORRES, Gabriel. **Criptografias**. Disponível em: <<http://www.clubedohardware.com.br/artigos/667>>. Acesso em 20 de mar. 2010.
- TRIGO, Clodonil Honório. **OpenLDAP: uma abordagem integrada**. São Paulo: Novatec Editora, 2007.
- VASCONCELOS, René. **Segurança Wireless, qual usar?**. Disponível em: <<http://bloglinksysbrasil.com.br/seguranca-wireless-qual-utilizar/>>. Acesso em 24 de abr. 2010.
- WIKIPEDIA. **WPA2 (AES)**. Disponível em: <[http://pt.wikipedia.org/wiki/WPA2\\_%28AES%29](http://pt.wikipedia.org/wiki/WPA2_%28AES%29)>. Acesso em 20 de mar. 2010.
- \_\_\_\_\_. **WPA**. Disponível em: <<http://pt.wikipedia.org/wiki/Wpa>>. Acesso em 20 de mar. 2010.
- \_\_\_\_\_. **TKIP**. Disponível em: <<http://pt.wikipedia.org/wiki/TKIP>>. Acesso em 21 de ago. de 2010.