CENTRO UNIVERSITÁRIO FEEVALE

RICARDO DALMORO BASSO

ANÁLISE DE VULNERABILIDADE DE REDE SEM FIO 802.11: UM ESTUDO DE CASO EM UM ORGÃO PÚBLICO MUNICIPAL

Anteprojeto de Trabalho de Conclusão

Novo Hamburgo, Setembro de 2008.

RICARDO DALMORO BASSO

rdbasso@gmail.com

ANÁLISE DE VULNERABILIDADE DE REDE SEM FIO 802.11: UM ESTUDO DE CASO EM UM ORGÃO PÚBLICO MUNICIPAL

Centro Universitário Feevale
Instituto de Ciências Exatas e Tecnológicas
Curso de Sistemas de Informação
Anteprojeto de Trabalho de Conclusão

Professor orientador: Vandersilvio da Silva

Novo Hamburgo, Setembro 2008.

RESUMO

Devido à crescente necessidade por mobilidade houve uma vasta expansão das redes sem fio, sendo estas, tecnologias que oferecem a promessa de transferência de dados cada vez mais rápidas e de baixo custo através de ligações bastante abrangentes. Muito se tem alcançado no que se diz respeito a montar ou controlar estas redes, mas as ferramentas fundamentais que permitem a confiabilidade e a autenticidade dos dados transportados ainda não estão bem explicadas. Comunicação sem fio no que diz respeito à segurança ainda é um enorme desafio para investigação. Os protocolos conhecidos hoje no mercado e que são atualmente os mais utilizados para segurança de redes sem fio são o WEP e o WPA. Diversos problemas com estes protocolos já são conhecidos. O presente trabalho pretende aprofundar os estudos no que diz respeito a confiabilidade destes protocolos, bem como avaliar sua eficiência e a devida proteção oferecida.

Palavras-Chave: Criptografia, Segurança, *Wireless*

SUMÁRIO

MOTIVAÇÃO

Com o avanço da comunicação nos últimos anos, a todo o momento, estão surgindo novas tecnologias de redes wireless, visando a atender as necessidades dos usuários com a melhor qualidade de transferência e segurança possíveis. Ao longo do tempo muito se evoluiu até chegar às redes de computadores da atualidade. As empresas e universidades estão apostando cada vez mais nesta tecnologia considerada revolucionária.

O crescimento da tecnologia *wireless* em ambientes empresariais vem acontecendo de maneira rápida. Em 2007, segundo o Instituto Gartner, o uso desta modalidade de redes aumentaria cerca de 64% nas organizações. Entre os participantes da pesquisa 44% citaram que a mobilidade iria alavancar a produtividade. Apesar do aumento do numero de adeptos as redes sem fio, 70% dos entrevistados relataram que não utilizam nenhum tipo de proteção contra invasores. Logo, a segurança torna-se o maior motivo de preocupação. http://www.silicon.com/

Quando o autor deste estudo ingressou em seu curso superior no ano de 2001, pouco se falava em conexões sem fio, tão pouco poderia prever a vasta expansão destes ambientes. Atualmente encontramos pontos de acesso *wireless* nos mais variados espaços sociais, desde o Aeroporto Internacional, até as praças públicas. O baixo custo e a qualidade do sinal oferecido tornam-se um grande atrativo para disseminar esta tecnologia.

Atualmente o autor atua profissionalmente em uma Prefeitura Municipal do interior do Estado, onde muito se fala em cidade digital - a qual é compreendida por uma conexão de alta velocidade que chega a um ponto, via link de uma operadora de telefonia, e se distribui no município por uma rede sem fio a lugares como escolas, postos de saúde e órgão da administração municipal. Diversos tipos de informações trafegam diariamente por essas redes,

transmitindo desde dados confidenciais como folha de pagamento dos colaboradores e prontuários médicos, como simples arquivos de e-mail.

Estas redes sem fio, de fácil montagem e simples configuração, levantam uma dúvida quando se pensa em sigilo dos dados trafegados. O mercado atual disponibiliza diversos modelos de equipamentos, de diversos fabricantes. Todos estes, tendo como seus protocolos padrões de segurança WEP e WPA.

Redes *wireless* podem usar criptografia para proteger o tráfego entre a estação cliente e a base. Este ponto de acesso pode ser configurado para usar uma chave autenticadora que é armazenada e transmitida quando o cliente tenta se conectar. A maioria esmagadora das redes sem fio utiliza como protocolo de segurança o WEP, que suas falhas já são conhecidas e com algumas descobertas recentes permitiram que passassem de horas para minutos o tempo levado para sua quebra.

> Existem várias ferramentas desenvolvidas para descobrir chaves WEP, com maior ou menor grau de eficiência. Utilizam, em geral, uma combinação de força bruta, ataques baseados em dicionário e exploração de vulnerabilidades conhecidas. Por outro lado, chaves simples são mais fáceis de ser quebradas, independentemente da eficácia da ferramenta, e chaves-padrão não necessitam sequer de ferramentas para isso. (RUFINO, 2005 p.101)

Tendo em vista estes já divulgados problemas de segurança, o protocolo WEP caiu em descrédito. Antes do fechamento do padrão 802.11i o wi-fi Alliance liberou o protocolo WPA. Diversas mudanças e avanços foram incorporados a este novo protocolo, além de possuir diversos modelos que são moldáveis as necessidades do ambiente.

> Grande parte do problema de sigilo existente no WEP diz respeito aos mecanismos de criptografia utilizados. Para solucionar esses problemas, o WPA avança nos pontos mais vulneráveis, quais sejam a combinação de algoritmo e temporalidade da chave. Porém, dados a diversidade e os ambientes onde uma rede sem fio pode existir (ambientes domésticos, pequenos escritórios, pequenas e grandes indústrias etc.), pensou-se ser razoável que o WPA tivesse também diferentes modelos de segurança para ter melhor aderência às diferentes necessidades. (RUFINO, 2005 p.35)

Embora o protocolo WPA seja mais seguro que seu antecessor WEP, algumas vulnerabilidades de seu método já são conhecidas nos dias de hoje, e estão reportadas em artigos e sites de busca na internet. É muito importante para seus adeptos, que sejam conhecidas estas informações para que possam se precaver em caso de qualquer tentativa de invasão. Entretanto até onde os dados criptografados por estas ferramentas estão realmente seguros? È possível garantir a integridade destas informações?

Motivado por estas indagações, este presente projeto de pesquisa será constituído de um estudo nos protocolos WEP e WPA, descrevendo suas vulnerabilidades e fazendo um comparativo entre eles. Além deste estudo pretende-se, efetuar uma tentativa de invasão ou simples quebra de criptografia com ferramentas adequadas, na rede já existente no ambiente *wireless* da cidade digital.

OBJETIVOS

Objetivo Geral

O presente projeto de pesquisa tem como objetivo principal analisar a vulnerabilidade da segurança em uma rede sem fio. Para tanto, será realizado um estudo bibliográfico e posteriormente um experimento em ambiente real, o qual proporcionará uma verdadeira idéia de proteção para a rede observada.

Objetivos Específicos

- Apresentar as características e descrever os protocolos WEP e WPA;
- Pesquisar e descrever como funcionam as técnicas e ferramentas para análise de vulnerabilidade de redes sem fio;
- Gerar relatórios para melhor visualização da pesquisa;
- Analisar os resultados obtidos;
- Propor um modelo de relatório de Analise de Vulnerabilidade.

METODOLOGIA

O estudo será estruturado em duas etapas: a primeira delas será o TCC1, composto pela fundamentação teórica dos protocolos que serviram de base para este projeto; pretende-se ainda, pesquisar e descrever como funcionam as técnicas e ferramentas para quebra de segurança. Como método, será realizado aprofundamento bibliográfico com base em livros doutrinários e pesquisas virtuais.

A segunda etapa consistirá em descrever o ambiente do experimento e a forma de realização do mesmo, bem como o material necessário para o desenvolvimento das tarefas. Concomitantemente, as ferramentas serão aplicadas na rede em questão e colhidos os resultados. Posteriormente, serão gerados relatórios analíticos destes estudos os quais contribuirão para a conclusão do trabalho realizado. Por último, pretende-se propor um modelo de relatório para analise de vulnerabilidade.

Etapa - TC1

- Entregar o aceite de Orientação;
- Pesquisar bibliografia específica;
- Revisar os conteúdos;
- Revisar projeto junto ao orientador;
- Elaborar o Ante-Projeto;
- Estudar os protocolos de segurança;
- Estudar, descrever e avaliar as técnicas e ferramentas para análise de vulnerabilidade;

- Elaborar o Trabalho de Conclusão I;
- Entregar o Trabalho de Conclusão I.

Etapa - TC2

- Revisar os conteúdos;
- Estudar e descrever o ambiente;
- Realizar o experimento com as ferramentas;
- Revisar projeto junto ao orientador;
- Gerar relatórios;
- Analisar os resultados obtidos;
- Propor um relatório de analise de vulnerabilidade;
- Elaborar o Trabalho de Conclusão II;
- Entregar o Trabalho de Conclusão II;
- Apresentar o trabalho para banca avaliadora.

CRONOGRAMA

Trabalho de Conclusão I

Etapas	Meses			
	AGO	SET	OUT	NOV
Entregar o aceite de Orientação;				
Pesquisar bibliografia específica;				
Revisar os conteúdos;				
Revisar projeto junto ao orientador;				
Elaborar o Ante-Projeto;				
Estudar os Protocolos de Segurança;				
Estudar, descrever e avaliar as técnicas e ferramentas para análise de vulnerabilidade;				
Elaborar o Trabalho de Conclusão 1;				
Entregar o TCC1.				

Trabalho de Conclusão II

Etapas	Meses			
	MAR	ABR	MAI	JUN
Revisar os conteúdos;				
Estudar e descrever o ambiente;				
Realizar o experimento com as ferramentas				
Revisar projeto junto ao orientador;				
Gerar relatórios;				
Analisar os resultados obtidos;				
Propor um relatório para analise de vulnerabilidade;				
Elaborar o Trabalho de Conclusão 2;				
Entregar o TCC2;				
Apresentar o trabalho para banca avaliadora.				

BIBLIOGRAFIA

EARLE, Aaron E. **Wireless Security Handbook**. United States of America: Auerbach Publications, 2006. 354p.

PRODANOV, Cleber Cristiano. **Manual de metodologia científica.** 3.ed. Novo Hamburgo: Feevale, 2006. 77 p.

ROSS, John. **Wi-Fi – Instale, configure e use redes wireless (sem fio)**. Rio de Janeiro: Alta Books, 2003. 246p.

RUFINO, Nelson Murilo de Oliveira. **Segurança em Redes sem Fio**. 2.ed. São Paulo: Novatec, 2005. 224p.

WIKIPÉDIA, **Wireless**, Disponível em <http://pt.wikipedia.org/wiki/Wireless>. Acesso em 1 de Setembro de 2008.

WI-FI Alliance. **Wi-Fi standards**. Disponível em <http://www.wi-fi.org > Acesso em: Setembro de 2007.