UNIVERSIDADE FEDERAL DA GRANDE DOURADOS

EDILENE VIRGULINA CARDOSO

TESTES DE FORÇA BRUTA EM PROTOCOLOS DE CRIPTOGRAFIA DE REDES WIRELESS

DOURADOS – MS
2009

EDILENE VIRGULINA CARDOSO

TESTES DE FORÇA BRUTA EM ALGORITMOS DE CRIPTOGRAFIA DE REDES WIRELESS

Trabalho de Conclusão de Curso de graduação apresentado para obtenção de título de Bacharel em Análise de Sistemas. Faculdade de Ciências Exatas e Tecnologia Universidade Federal da Grande Dourados Orientador: Professor M. Sc. Marcos Paulo Moro.

DOURADOS – MS
2009

EDILENE VIRGULINA CARDOSO

TESTES DE FORÇA BRUTA EM ALGORITMOS DE CRIPTOGRAFIA DE REDES WIRELESS

Trabalho de Conclusão de Curso aprovado como requisito parcial para obtenção do titulo em Bacharel em Analise de Sistemas na Universidade Federal da Grande Dourados, pela comissão formada por:

Orientador: Prof: M. Sc. Marcos Paulo Moro
FACET-UFGD

Prof. Dr. Adailton José Alves da Cruz
FACET – UFGD

Prof. M. Sc Rodrigo Porfírio da Silva Sacchi
FACET-UFGD

Dourados, 23 de dezembro de 2009

AGRADECIMENTOS

Aos meus pais Arcenio e Helena, que me apoiaram e me ajudaram em todos os momentos de necessidade. Aos meus irmãos Erci, Julio César e Reinaldo, que acompanharam minha longa caminhada e muitas vezes me socorreram em momentos de apuro. Ao meu orientador, Professor M. Sc. Marcos Paulo Moro, o qual me acompanhou e não me deixou desistir, inclusive emprestou seus equipamentos pessoais para os experimentos realizados neste trabalho. E acima de tudo, tenho que agradecer ao meu bom DEUS, que me iluminou, ouviu minhas suplicas e colocou suas mãos abençoadas sobre mim.

RESUMO

O crescimento das redes sem fio (*Wireless Network*) pelo mundo introduz provisão de qualidade de serviço, o que está estreitamente condicionada à questão da segurança. A segurança em seu ponto principal encontra-se defeituosa no que diz respeito à segurança integral das redes sem fio, pois invasões nos mais variados formatos foram constatadas. Essa deficiência motiva o estudo sobre protocolos de segurança utilizados em redes sem fio, logo foram feitas análises dos mecanismos de segurança com suas respectivas vantagens e desvantagens de utilização, buscando obter segurança e a integridade das informações que trafegam na rede. Esses protocolos utilizam técnicas de criptografia para alcançar seus objetivos, tais como, sigilo, autenticação e integridade dos dados, entretanto, esses protocolos criptográficos estão sujeitos a erros no seu desenvolvimento, tornando-os vulneráveis a ataques. Os protocolos de destaque nesse trabalho são *WEP, WPA e WPA2*. Este trabalho busca a enforcar a maneira pela qual a encriptação e desencriptação dos dados são realizados, os algoritmos utilizados, e onde ocorre à falha nos protocolos estudados. Ao final da pesquisa, foram realizados testes práticos, demonstrando as vulnerabilidades, fragilidades e como pode ser feita a quebra da chave utilizando ferramentas de ataques encontradas na Internet. Por fim, é descrito os tipos de senhas que devem ser usadas, em *redes wireless,* visando bloquear o acesso a rede por pessoas não autorizadas.

Palavras chaves: Protocolos de segurança, Redes *Wireless*, Segurança em redes sem fio, Quebra de chave.

ABSTRACT

The growth of wireless networks (Wireless Network) introduces the world supply of quality service, which is closely determined the issue of security. Security on your main point is flawed with regard to integral security of wireless networks, for invasions in various formats were found. This deficiency motivates the study of security protocols used in wireless networks, then were analyzed in the security arrangements with their respective advantages and disadvantages of use, seeking to obtain security and integrity of information that travels on the network. These protocols use cryptographic techniques to achieve their goals, such as confidentiality, authentication, data integrity, however, these cryptographic protocols are subject to errors in its development, making them vulnerable to attack. Protocols in this work are highlighted WEP, WPA and WPA2. This paper seeks to hang the manner in which encryption and decryption of data are performed, the algorithms used, and where the failure occurs in the protocols studied. At the end of the study, practice tests were performed, demonstrating the vulnerabilities, weaknesses and how it can be done to break the key attacks using tools found on the Internet. Finally, we describe the types of passwords that must be used in wireless networks, in order to block network Access by unauthorized persons.

Key words: Security Protocols, Wireless Networks, Security in wireless networks, break key.