

Resumo

A segurança em sistemas informáticos é um tema actual e que suscita bastante interesse na comunidade informática em geral e nos responsáveis pela instalação e administração de sistemas/servidores em particular. Dada a enorme utilização de redes de computadores e a disseminação exponencial da Internet e da oferta cada vez maior de serviços sobre a Internet, torna-se fulcral o estudo, a aplicação e a avaliação de servidores seguros que, suportando estes serviços, permitam aos seus administradores um nível elevado de confiança na segurança dos mesmos.

Neste sentido, este trabalho apresenta um estudo sistemático e didáctico sobre o tema genérico da segurança em sistemas informáticos, e sobre as tecnologias e ferramentas mais utilizadas na implementação de servidores Linux com um grau superior de segurança. Inicialmente apresentam-se as metodologias utilizadas no planeamento de sistemas seguros, posteriormente abordam-se as ameaças mais relevantes e, por fim, identificam-se as ferramentas de segurança que melhor se adequam à defesa do servidor Linux.

Para completar este estudo, procedeu-se à instalação/implementação de um servidor Linux que integra as ferramentas estudadas mais adequadas e que lhe conferem as características superiores de segurança procuradas. Posteriormente, analisam-se as ferramentas disponíveis para que os administradores do sistema possam realizar testes e monitorizar o estado do sistema, conferindo-lhe assim um maior grau de confiança no sistema. Finalmente, apresenta-se um conjunto de testes que permitiram avaliar a eficácia dos mecanismos de segurança implementados no servidor.

Abstract

The computer system's security is a contemporary topic which raises the interest of the computer science community in general and the system's/server's administrators in particular. Given the enormous use of computer networks and the exponential spread of the Internet and the increasing offer of services over the Internet, it becomes vital the study, implementation and evaluation of secure servers for supporting these services, enabling their administrators to have a high level of confidence in the safety of their systems.

In this sense, this work presents a systematic and didactic study about the general subject of security in computer systems, and also about the latest tools and technologies used in the implementation of Linux servers with a higher degree of security. Initially, this project presents the methodologies used for planning secure systems, then it address the most relevant threats and, finally, it identifies the security tools that are best suited for defending the Linux server.

To complete this study, the author installed/implemented a Linux server that integrates a selection of the most appropriate tools studied which grant it the pursued higher security features. Afterwards, we examine the available tools that the system administrators can use to perform tests and monitor the state of the system, thereby giving him a greater degree of confidence in the system. Finally, we present a series of tests that allowed assessing the effectiveness of the security mechanisms implemented on the server.