

UM LEVANTAMENTO BIBLIOGRÁFICO SOBRE TÉCNICAS E FERRAMENTAS LIVRES PARA SEGURANÇA DE SERVIDORES LINUX

Hyago Sayomar Dias Ferreira
Guilherme Álvaro Rodrigues Maia Esmeraldo

Resumo: Há muito tempo o GNU/Linux foi considerado um “azarão”, sendo escolhido apenas por aqueles que buscavam Sistemas Operacionais alternativos. Contudo, esse sistema cresceu e amadureceu, e hoje vem sendo requisitado por apresentar alto desempenho, estabilidade e segurança, sendo frequentemente encontrado em aplicações de servidores computacionais. No entanto, sabe-se que não há sistema totalmente seguro. Nesse contexto, o presente trabalho tem por objetivo apresentar as possíveis vulnerabilidades, tanto físicas quanto lógicas, existentes em servidores GNU/Linux, bem como as principais técnicas e ferramentas livres para fortalecer sua segurança. Este trabalho buscou ainda realizar uma análise aprofundada de diferentes ferramentas e sua documentação, em formato de manual de boas práticas, para uso por aqueles que necessitam implementar aspectos de segurança em servidores GNU/Linux. Para o desenvolvimento do trabalho, empregou-se o método de revisão bibliográfica, para levantamento e análise de referências bibliográficas – livros e artigos, principalmente – relacionadas aos temas de Segurança da Informação e Servidores GNU/Linux. No trabalho final, apresenta-se uma breve discussão sobre segurança da informação, seguida das principais vulnerabilidades existentes em servidores GNU/Linux e, por fim, lista-se e descreve-se as ferramentas e um conjunto de técnicas para fortalecer a segurança nesses servidores. Os trabalhos futuros consistem em aperfeiçoar o trabalho aqui descrito com a inclusão de novos recursos e técnicas do estado da arte nas áreas correlatas.

Palavras-chave: Sistema Operacional. Servidor Computacional. GNU/Linux. Segurança da Informação.

Referências

- ANÔNIMO, **Segurança Máxima para Linux**. Rio de Janeiro: Editora Campus Ltda, 2000.
- MORIMOTO, CARLOS E. **Manual do Hardware Completo 3ºed**. GDH Press e Sul Editora, 2007.
- MELO, Sandro. **BS7799 Linux da Tática à Prática em Servidores**. São Paulo: Alta Books, 2006.
- MELO, Sandro. **Exploração de Vulnerabilidades em Redes TCP/IP** / Sandro Melo. - 3.ed. - Rio de Janeiro: Alta Books, 2017.
- WEIDMAN, Georgia. **Teste de Invasão: Uma Introdução Prática ao Hacking**. - 1.ed. - São Paulo: Novatec Editora Ltda, 2017.