

#### SECURITYDOG: SCRIPT DE HARDENING PARA SERVIDORES GNU/ LINUX DEBIAN

CAIRO APARECIDO CAMPOS ANTONIO EDUARDO MARQUES DA SILVA





## Relevância do Estudo

- Servidores mal configurados → Exploração de vulnerabilidades;
- Servidor invadido → Porta de entrada;
- Indisponibilidade de um servidor, roubo de dados e o comprometimento de um banco de dados:
  - Perda financeira e de competitividade;
  - Falência do negócio.
- Impedir/dificultar a invasão de servidores → Técnicas de hardening
  - Definição do termo
  - Exemplos de técnicas



### **Objetivos**

- Desenvolver um script de hardening, afim de facilitar, automatizar e diminuir o tempo gasto na realização de configurações de segurança em servidores GNU/Linux Debian;
- Utilizar o script como um roteiro de melhores práticas a ser seguido, para diminuir vulnerabilidades de um sistema após a sua instalação.



Fonte: http://b4.net.br/noticias/definindometas-e-objetivos-alcancaveis



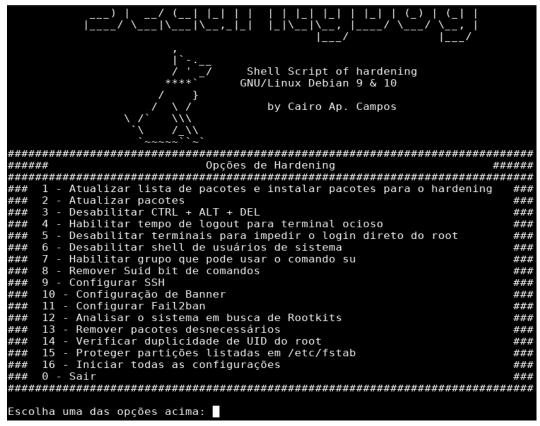
# Aspectos Metodológicos

- O script SecurityDog foi desenvolvido utilizando a linguagem shell script e o interpretador de comandos bash;
- O script foi testado na versão 9 (oldstable) e na versão 10 (stable) do GNU/Linux Debian;
- O SecurityDog é licenciado pela GNU GPL v3 e pode ser encontrado no link abaixo do repositório do GitHub:

https://github.com/cairoapcampos/SecurityDogV1



### Aspectos Metodológicos



Fonte: autor (2019)



## Discussão e/ou Análise dos Resultados



Fonte: https://oenem.com.br/blog/resultados/page/2/



# Considerações Finais e Trabalhos Futuros

- O script desenvolvido possibilitou um roteiro de melhores práticas a ser seguido para o fortalecimento de um servidor GNU/Linux Debian após sua instalação;
- Para uma melhor eficiência, este roteiro deve ser utilizado em conjunto com outras práticas de segurança;
- Trabalhos futuros:
  - Adicionar no script a opção de hardening port knocking, que também é utilizada para proteger o SSH;
  - Definir configurações de hardening para os serviços Apache, MySQL, BIND, entre outros.





