

Segurança da Informação

Prevenção de Ataques e Defesas
Utilização do Kali Linux

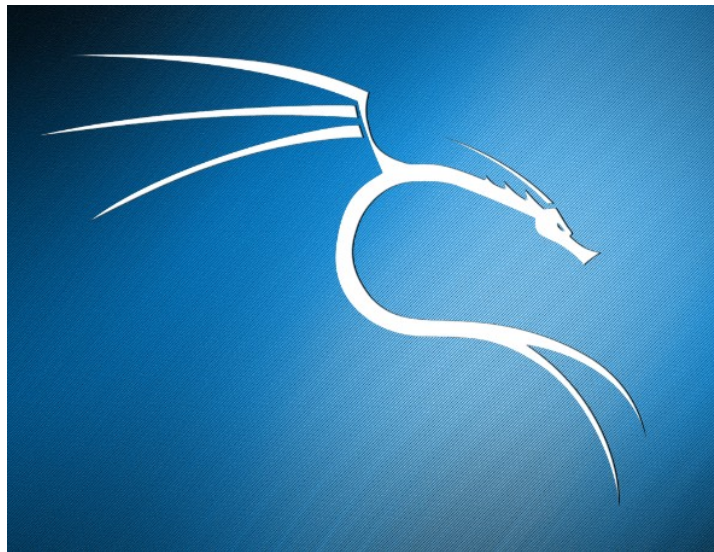
Prof. Fábio Henrique Ribeiro Machado
fabiohenriquerm@gmail.com



O que é Kali Linux

Kali Linux é uma avançada distribuição Linux especializada em Testes de Intrusão e Auditoria de Segurança.

<https://www.kali.org/>



Funcionalidades do Kali

Kali é uma reconstrução completa do BackTrack Linux, que adere totalmente aos padrões de desenvolvimento do Debian.

Uma infraestrutura completamente nova foi montada, todas as ferramentas foram revistas e empacotadas, e utiliza Git como nosso Sistema de Controle de Versões.



Funcionalidades do Kali

- **Mais de 300 ferramentas de testes de intrusão:** Depois de rever cada ferramenta que estava incluída no Backtrack, eliminamos um grande número de ferramentas que não funcionavam, ou para as quais havia outra ferramenta com funcionalidade semelhante;
- **É, e sempre será gratuito:** Kali Linux, como seu predecessor, é completamente livre, e sempre permanecerá como tal. Você nunca, nunca terá que pagar pelo Kali Linux;
- **Repositório Git livre:** Somos proponentes convictos do software de código aberto e nosso repositório está disponível para todos que todos vejam e todos os fontes estão disponíveis para aqueles que desejem adaptar e remontar os pacotes;



Funcionalidades do Kali

- **Complacente com o padrão FHS:** Kali foi desenvolvido para aderir ao Padrão Hierárquico do Sistema de Arquivos (ou FHS da sigla em inglês), permitindo que todos os usuários Linux facilmente localizem arquivos binários, de apoio, bibliotecas, etc;
- **Vasto suporte à dispositivos wireless:** Construimos o kali Linux para suportar tantos dispositivos wireless quanto pudemos, permitindo que o mesmo executasse adequadamente numa vasta gama de hardware e o tornando compatível como diversos outros dispositivos sem fio e USB;



Funcionalidades do Kali

- **Kernel adaptado para injeção de pacotes:** Como consultores de testes de intrusão, a equipe de desenvolvimento às vezes precisa fazer avaliações em redes sem fio, então nosso kernel já inclui os últimos patches de injeção de pacotes.
- **Repositórios e pacotes com assinaturas GPG:** Todos os pacotes do Kali são assinados por cada desenvolvedor individual quando eles são construídos e submetidos ao repositório, que em seguida assina os pacotes também.



Funcionalidades do Kali

- **Múltiplos idiomas:** Embora as ferramentas usadas em testes de intrusão tendam a ser escritas em inglês, nós nos asseguramos que o Kali possuísse um suporte a idiomas real, permitindo que mais usuários o operassem no seu idioma nativo, e encontrasse as ferramentas de que precisa para realizar suas tarefas.
- **Totalmente customizável:** Nós entendemos perfeitamente que nem todos irão concordar com nossas decisões de design, então tornamos o mais fácil possível que nossos usuários mais aventureiros o customizem o Kali Linux ao seu gosto, através de todo o sistema até o kernel.



Funcionalidades do Kali

- **Suporte à ARMEL e ARMHF:** Já que os sistemas baseados em processadores ARM estão se tornando mais e mais presentes e baratos, sabíamos que o suporte a processadores ARM no Kali precisaria ser o tão robusto quanto pudéssemos gerenciar, o que resultou em instaladores funcionais tanto para sistemas ARMEL quanto para ARMHF. Kali Linux tem repositórios ARM integrados com a distribuição principal, então ferramentas para ARM serão atualizadas em conjunto com o resto da distribuição.



Funcionalidades do Kali

Kali atualmente está disponível para os seguintes dispositivos ARM:

rk3306 mk/ss808

Raspberry Pi

ODROID U2/X2

Samsung Chromebook

Kali é especialmente indicado para testes de intrusão, então toda a documentação deste site pressupõe um conhecimento anterior do sistema operacional Linux.

