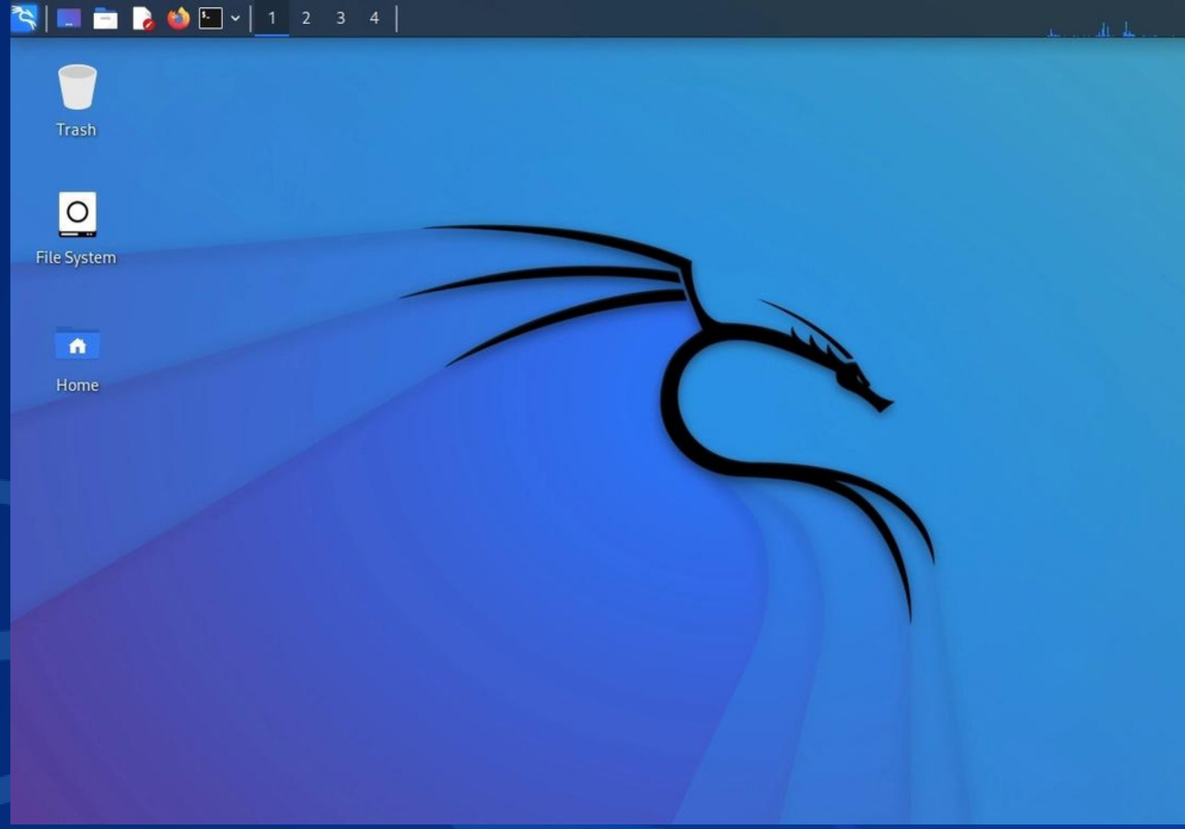
LINUX
KALI

EQUIPE 5 - TYP

O QUE É O KALI?

O Kali (anteriormente conhecido como BackTrack Linux) é uma distribuição Linux de código aberto, baseada no Debian, voltada para testes avançados de penetração e auditoria de segurança.

O Kali tem aproximadamente **600** programas de teste de penetração, incluindo:
Armitage (uma ferramenta gráfica de gerenciamento de ataques cibernéticos),
Nmap (um scanner de porta),
Wireshark (um analisador de pacotes),
metasploit (estrutura de teste de penetração),
John the Ripper (um cracker de senhas), s
qlmap (ferramenta automática de injeção de SQL e aquisição de banco de dados), entre outros...



Também é uma solução multiplataforma, acessível e disponível gratuitamente para profissionais e amadores de segurança da informação.

ESPECIFICAÇÕES

MÍNIMAS:

Mínimo de 20 GB de espaço no HD.

Processador de 1GHz ou superior.

Mínimo de 2 GB de RAM.

Unidade de CD-DVD inicializável ou um pendrive USB.

RECOMENDADAS:

Mínimo de 50 GB de espaço no HD, de preferência SSD

Processador de 2GHz ou superior.

Pelo menos 4 GB de RAM

Unidade de CD-DVD inicializável ou um pendrive USB.

QUAL A SUA UTILIDADE?

TESTES DE SEGURANÇA E PENETRAÇÃO:
O Kali é projetado para fazer testes de segurança em sistemas, redes e aplicativos.

ANÁLISE FORENSE DIGITAL:
Ele possui ferramentas e recursos para análise forense digital, que são usados para coletar evidências digitais e recuperar informações de sistemas comprometidos.

AUDITORIA DE SEGURANÇA:
O Kali oferece ferramentas para avaliar a segurança de configurações de rede, identificar vulnerabilidades, verificar padrões de segurança e realizar teste de stresse em infraestruturas de TI.

TREINAMENTO E EDUCAÇÃO:
O Kale também tem um ambiente prático para aprender e praticar técnicas de segurança, testes de penetração e análise forense digital.

CÓDIGO ABERTO:
O Kali Linux é baseado em código aberto, ou seja, a comunidade de desenvolvedores pode contribuir e aprimorar constantemente suas ferramentas e recursos. Isso faz com que uma ampla gama de ferramentas de segurança e recursos atualizados e mantidos pela sua comunidade.

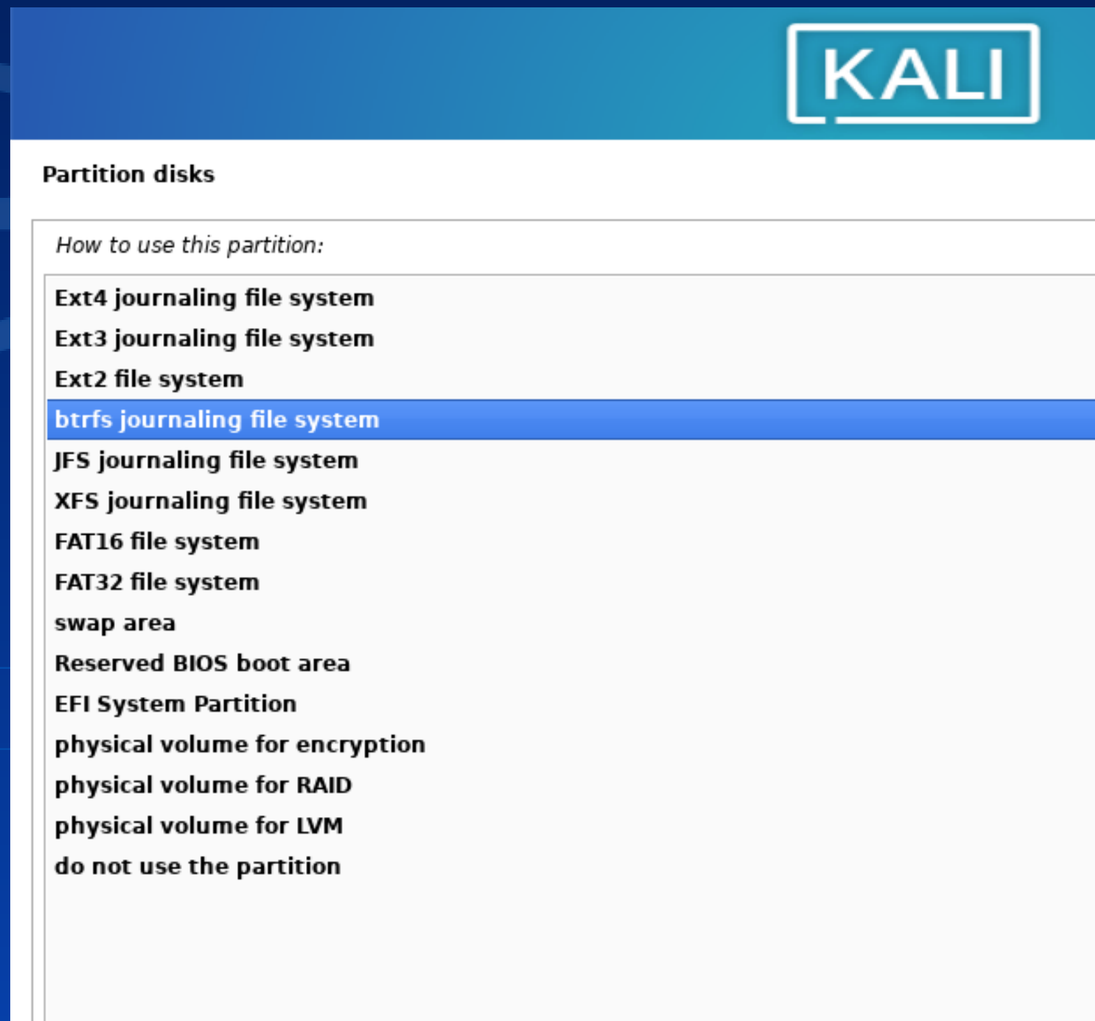
QUAIS SISTEMAS DE ARQUIVOS ELE UTILIZA?

Na instalação do Linux Kali, tem opção de selecionar mais de 8 tipos de sistema de arquivos, entre eles:

Ext2 (second extended file system):
Foi inicialmente desenvolvido para substituir o ext, e foi o primeiro sistema de arquivos de nível comercial para Linux.

EXT3 (THIRD EXTENDED FILESYSTEM):
Sua principal vantagem sobre o ext2 é o registro, o que melhora a confiabilidade e elimina a necessidade de verificar o sistema de arquivos após um desligamento não limpo.

EXT4 (FOURTH EXTENDED FILESYSTEM):
Foi projetado para suportar volumes e arquivos individuais muito grandes. Também apresenta recursos avançados que melhora muito o desempenho do disco.



BTRFS (B-TREE FILE SYSTEM):
Projetado para solucionar problemas como falta de agrupamento de discos ou volumes, snapshots, checksums, e uso de múltiplos volumes simultaneamente nos sistemas de arquivos do Linux.

JFS (JOURNALED FILE SYSTEM):
Sistema de arquivos de 64 bits com journaling desenvolvido pela IBM.

XFS:
Permite extrema escalabilidade de threads de E/S, largura de banda do sistema de arquivos e tamanho dos arquivos e do sistema de arquivos em si, ao abranger vários dispositivos de armazenamento físico.

FAT16 (FILE ALLOCATION TABLE)
O sistema de arquivos FAT-16 é utilizado pelos sistemas operacionais MS-DOS e Windows 95. Este sistema utiliza 16 bits para o endereçamento de dados.

FAT32 (FILE ALLOCATION TABLE)
A fim de superar o limite de tamanho de volume do FAT16, enquanto ao mesmo tempo permitir que o código em modo real do DOS lide com o formato, a Microsoft criou uma nova versão do sistema de arquivos, o FAT32, que suportava um maior número de clusters possíveis

PONTOS FORTES:

FERRAMENTAS DE SEGURANÇA:
O Kali é fornecido com uma ampla gama de ferramentas de segurança e testes de penetração, possuindo mais de 600 ferramentas.

ATUALIZAÇÕES REGULARES:
O Kali recebe atualizações regulares para manter as ferramentas e os pacotes atualizados. Importante para garantir que as vulnerabilidades e as ferramentas estejam em conformidade com os padrões mais recentes.

DOCUMENTAÇÃO ABRANGENTE:
O Kali possui uma documentação detalhada e abrangente, que inclui guias de instalação, tutoriais e explicações sobre o uso das ferramentas de segurança.

PONTOS FRACOS:

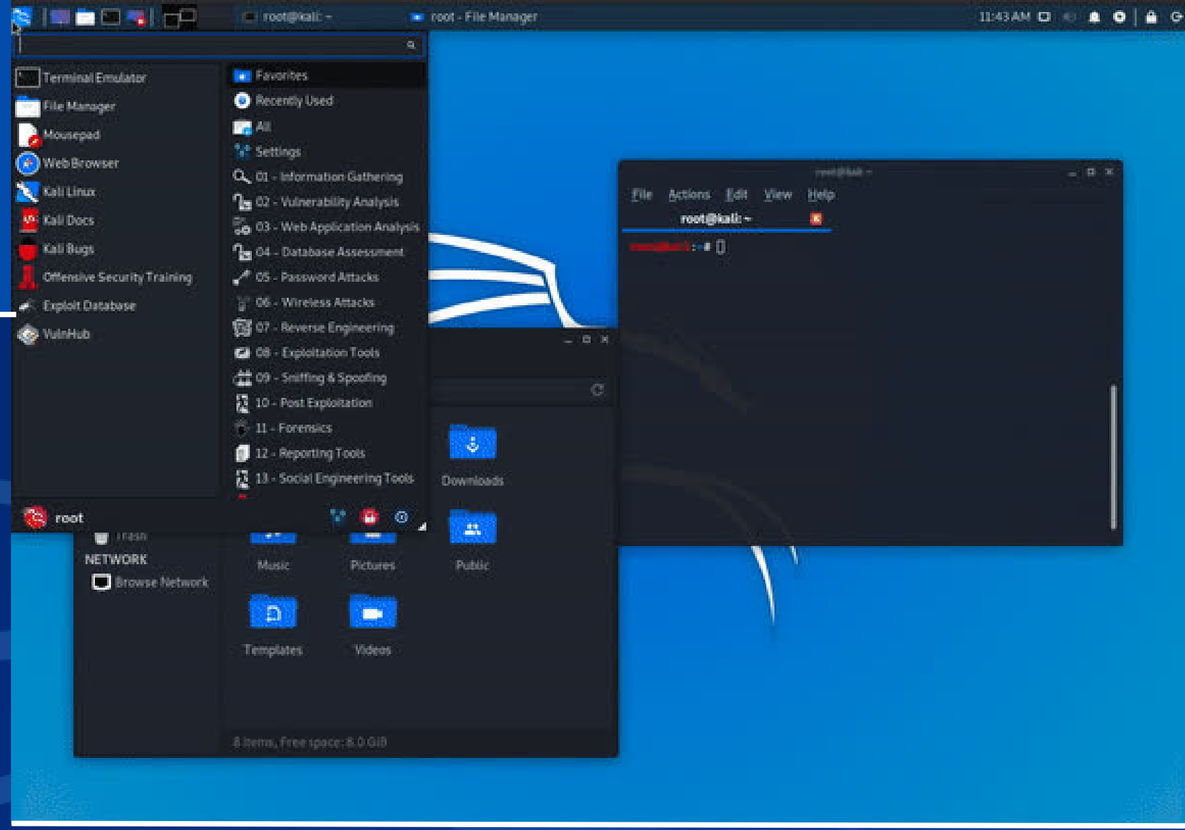
COMPLEXIDADE:
O Kali é uma distribuição avançada e voltada para usuários experientes em segurança e testes de penetração.

USO IMPRÓPRIO:
O Kali é uma poderosa ferramenta de segurança, mas também pode ser mal utilizada por hackers e todos os tipos de indivíduos mal-intencionados.

INCOMPATIBILIDADE COM HARDWARE:
Como o Kali é uma distribuição específica para testes de segurança, alguns dispositivos ou drivers de hardware podem não ser totalmente suportados.

CURIOSIDADES

O Kali teve participação na série **Mr. Robot**, desempenhando um papel fundamental nas atividades de hacking e segurança virtual retratadas na trama.



Ele tem uma função **"Kali Undercover"**, que transforma o ambiente de trabalho do linux em um idêntico ao do Windows 10.
Essa função tem como conceito:
Esconder-se em público.

GLOSSÁRIO

GLOSSÁRIO:
Conjunto de termos de uma área do conhecimento e seus significados, ou seja, uma explicação sobre os termos técnicos ou ou de outra língua usados em uma obra.

FORENSE DIGITAL:
É um ramo que abrange a recuperação e investigação de material encontrado em dispositivos digitais, geralmente em relação a crimes computacionais.

SNAPSHOT:
É uma cópia exata e completa do HD da sua máquina, virtual ou física, feita em um determinado momento. Se a recuperação de dados se fizer necessária, ele recupera todas as informações do disco até a data do snapshot.

REGISTRO (JOURNALING):
É um componente do sistema de arquivos que registra todas as alterações que ocorrem em informações sobre os arquivos e diretórios antes de serem aplicadas no sistema de arquivos propriamente dito. O objetivo principal do registro é evitar a corrupção de dados em caso de falhas ou interrupções repentinas no sistema.

AGRUPAMENTO DE DISCO (DISK CLUSTERING)
Refere-se à prática de combinar vários discos rígidos físicos em um único conjunto lógico. O objetivo principal do agrupamento de disco é melhorar o desempenho, a capacidade de armazenamento ou a confiabilidade do sistema de armazenamento.

TESTE DE PENETRAÇÃO: (͡° ͜ʖ ͡°)
Também conhecido como "pentest" ou "teste de intrusão", é um processo de avaliação da segurança de um sistema, rede, aplicativo ou infraestrutura de TI. O objetivo principal é identificar vulnerabilidades e pontos fracos que podem ser explorados por indivíduos mal-intencionados.

ENDEREÇAMENTO DE DADOS:
é o processo de atribuir uma localização específica a um conjunto de dados em um sistema de armazenamento. Isso permite que o sistema acesse e manipule os dados armazenados de forma eficiente.

CLUSTER:
Um cluster é uma coleção de setores de um disco, que é a menor unidade endereçável em um disco.

OBRIGADO!

DE TODA A EQUIPE TYP!

Kevin Henriques
Gustavo Faria Cardoso
Diogo Coraiola Guimarães
Enzo Ian Schnitzler Vieira
Pedro Lyra