Kali Linux

Débora Bianca & Ewelly Fabiane

Penetration Testing and Ethical Hacking Linux Distribution

kali.org

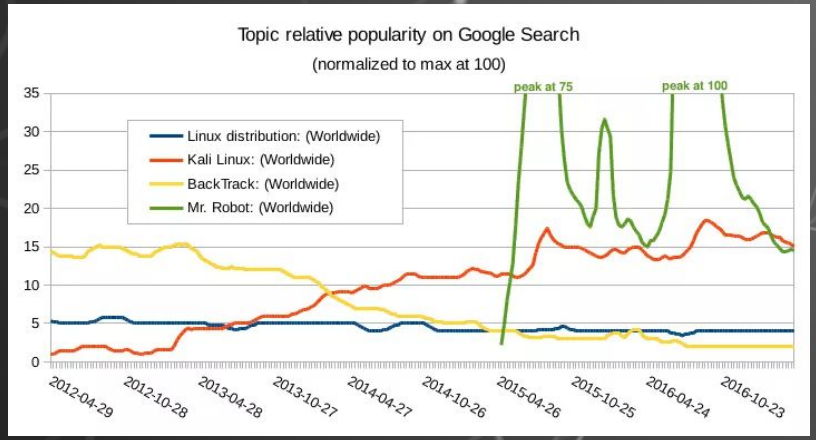
A ORIGEM

- Lançamento dia 13 de março de 2013;
- Desenvolvido pela Offensive Security;
- É uma distribuição GNU/Linux baseada no Debian e projetada para a forense digital e testes de penetração.
- O nome Kali tem como origem uma divindade do hinduísmo e sua etimologia significa “negra” ou “pele escura”.

KALI LINUX

SOBRE

- Versão atual: 4.19.0-kali5-amd64
- Open source;
- O próprio kali.org disponibiliza cursos sobre o Kali Linux;
- BackTrack (ubuntu) e Kali são essencialmente o mesmo;



Fonte: https://itsfoss.com/kali-linux-review/

INSTALAÇÃO

1º Inicializar com o meio de instalação;
2º Escolher o método de instalação;
3º Seleciona a líguagem;
4º Define o Local;
5º Insira um nome de host;
6º inserir o nome de um usuário não raiz para o sistema;
7º Definir fuso horário;
8º Selecionar o disco onde vai ser instalado;

Fonte:
https://sempreupdate.com.br/como-instalar-passo-a-passo-o-kali-linux-2019/

9º Seleciona o particionamento;
10º O disco que será particionado;
11º Decide se irá gravar as mudanças no gerenciador de volumes lógicos;
12º Configurar os espelhos de rede; (se selecionar “não”, você não poderá instalar pacotes de repositórios kali);
13º instalar o grub;
14º espere;

Pré-requisitos mínimos:
30GB no disco para instalação;
Ram para arquitetura i386 e amd64, no mínimo com 2GB;
Suporte de inicialização CD ou USB.

O DIFERENCIAL (PRE-PACKAGED)

Análise de Vulnerabilidade;

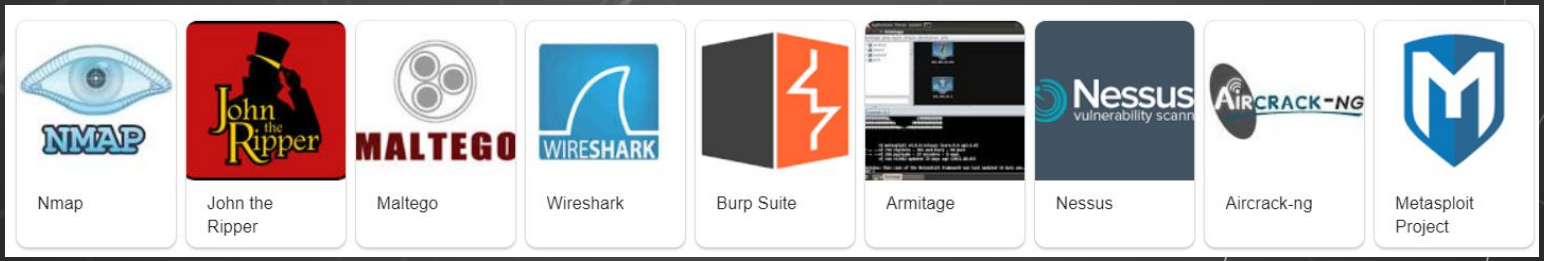
Ataques Wireless;

Ferramentas Forenses;

Hacking de Hardware;

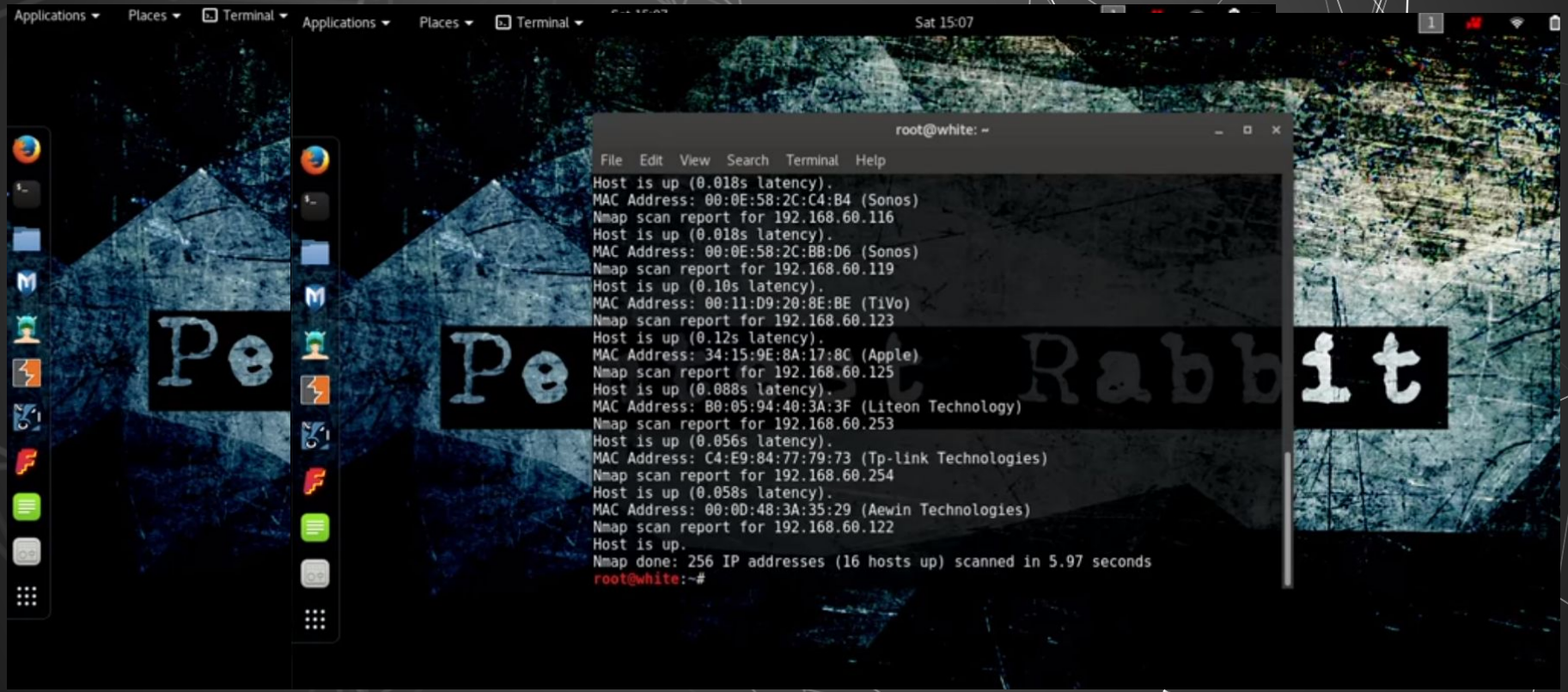
Fonte: https://tools.kali.org/tools-listing


01-Information
02-Vulnerability
03-WebApps
04-Database
05-Password
06-Wireless
07-Reversing
08-Exploit
09-Sniffing
10-PostExploit
11-Forensics
12-Reporting
13-SETools
14-Services
Ajuda
Ajustes
Analisador de u...
Arquivos
Calculadora
Caracteres
CherryTree
Chromium Nav...
Configuração a...
Configurações


Nmap
John the Ripper
Maltego
Wireshark
Burp Suite
Armitage
Nessus
Aircrack-ng
Metasploit Project

KALI APPLICATION (NMAP)

Fonte: https://www.youtube.com/watch?v=RH4Me0Acrz8



Formato de partições

- Todos os arquivos em uma partição só (para iniciantes);
- Partição /home separada;
- Partições /home, /var e /tmp separadas

Tabela 01:

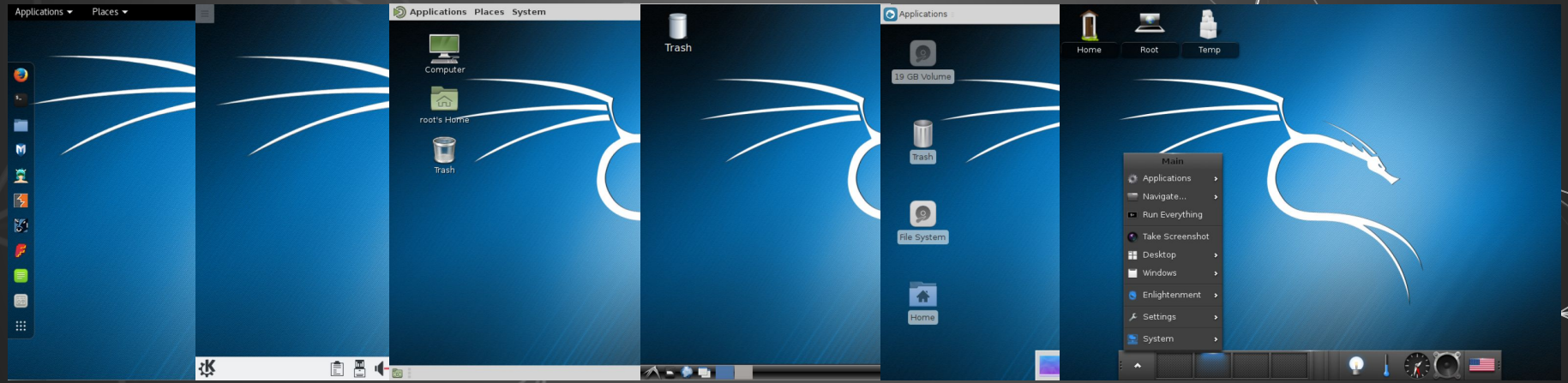
TAMANHO DO DISCO = 160 GB	TAMANHO CONSIDERADO PELO SISTEMA = 149,01 GB

RÓTULO	TIPO	SISTEMA DE ARQUIVOS	TAMANHO	ESTRUTURA DE DIRETÓRIOS
/boot	PARTIÇÕES PRIMÁRIAS	ext4	5.0 GB	Informações dos gerenciadores de inicialização;
/		ext4	30.0 GB	Principal diretório de um sistema GNU/Linux;
/root		ext4	10.0 GB	Diretório p/ centralizar dados usuais do superusuário root;
/swap	PARTIÇÕES LÓGICAS	==	5.0 GB	Memória virtual; (geralmente o dobro do tamanho da Ram)
/home		ext4	40.0 GB	Diretório p/ centralizar dados usuais dos usuários comuns;
/usr		ext4	30.0 GB	Mantém informações estáticas de aplicativos e serviços;
/opt		ext4	5.0 GB	Utilizado p/ instalar pacotes adicionais compilados;
/var		ext4	20.0 GB	Informações variáveis do sistema e de aplicativos em geral;
/tmp		ext4	5.0 GB	Armazena arquivos de ordem temporária;
/mnt		ext4	5.0 GB	Utilizado em pontos de montagem de uso temporário
/srv		ext4	5.0 GB	Informações estáticas de serviços disponibilizados pelo sistema

INTERFACES GRAFICAS

Lançadas em 2016.2:

- KDE, MATE, LXDE, Xfce, e17;



Fonte: https://fossbytes.com/kali-linux-2016-2-released-best-ethical-hacking-distro-multiple-flavours/

Modos de uso

Kali linux em uma unidade USB inicializável Kali

Instalando o Kali Linux

Kali Linux em ARM

Empresas e pessoas que utilizam a distro

Profissionais e estudantes da área de segurança

Estudantes que têm interesse nos recursos no modo root ou para fazer algum treinamento

Alunos do professor Herbert que precisam apresentar um seminário o Kali

Informações do kali

Versão do Kernel

```
root@kali:~# uname -r
4.19.0-kali1-amd64
```

Versão do gnome

```
root@kali:~# gnome-shell --version
GNOME Shell 3.30.1
```

BUGS

Estão sempre sendo corrigidos, alguns bugs ocorrem quando usuários leigos tentam usar o sistema para uso pessoal.

No Kali Linux 2018.3 foram adicionados correções para as vulnerabilidades de segurança Specter e Meltdown.

https://bugs.kali.org/view_all_bug_page.php

Gerenciamento de energia

Políticas baseadas no Debian, possui dois modos diferentes "com energia da bateria" e "com energia da tomada"

Seus recursos:

- monitoramento de bateria
- configurações de frequência de cpu
- configurações de DPMS do monitor
- suspender/hibernar
- controle de brilho de LCD
- controle das ações relacionados a ligar dormir e tela

ALÔ COMUNIDADE

- Possui 7 canais de comunicação (Blog, Fórum, Facebook, Twitter, IRC/documentação, Bug tracker e Feed RSS);
- Não fornece suporte a testes de penetração e nem ao uso das ferramentas;
- Dá suporte apenas em relação sistema operacional e aos problemas de empacotamento;

MÓDULO NO KERNEL