



SISTEMAS OPERACIONAIS · SEMINÁRIO

Parrot Security OS

Artur Bonamigo

Felipe Bueno

Gustavo Walter

O que é o ParrotOS

Distribuição GNU/Linux gratuita, baseada em Debian, para profissionais e estudantes de segurança, desenvolvedores e usuários que valorizam privacidade.

Uma base Linux completa + configurações de segurança + arsenal de ferramentas, tudo em um só sistema.

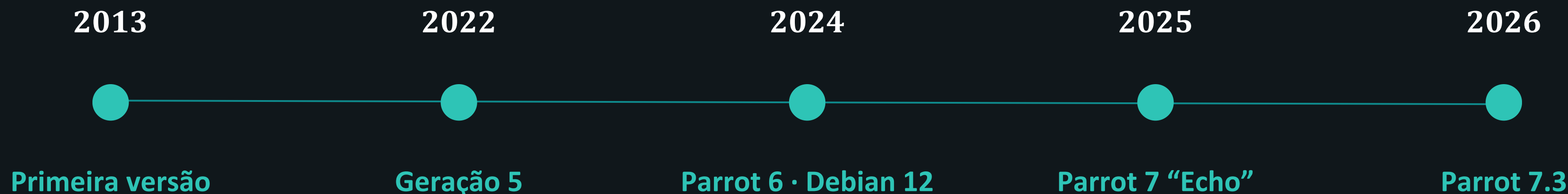
IDEIA CENTRAL

Não é só uma coleção de ferramentas de hacking.

É uma distribuição completa, pronta para fluxos de trabalho de cibersegurança.

Histórico

Primeira versão pública em 10 de abril de 2013, por Lorenzo Faletra, ligado à comunidade Frozenbox.



PARROT 7 “ECHO”

Passou a usar Debian 13 e KDE Plasma 6 com Wayland, mostra que o projeto também moderniza a própria plataforma, não só as ferramentas.

Lorenzo “Palinuro” Faletra

FORMAÇÃO

Engenharia Informática e de Telecomunicações
Università degli Studi di Palermo — 2015–2019

CARREIRA

Linux • Software • Cibersegurança

PARROT

Criador e líder do desenvolvimento desde 2013



Equipe Principal



Lorenzo Faletra
Palinuro

Cabeça de Papagaio



Nikos Fountas
NFOU

SVP de Operações na Hack The Box, Diretor e
Conselheiro Estratégico na Parrot Sec



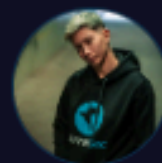
Emmanouil Gavriil
Arkanoid

VP de Conteúdo na Hack The Box e Diretor e
Consultor Estratégico na Parrot Sec



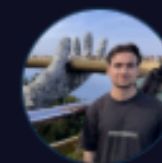
Dario Camonita
Danterolle

Engenheiro de Software Sênior II



Giulia M. Stabile
SH4RK

Diretor - Gerente de Marketing e Operações



Lefteris Dimitriou
Lefty

Engenheiro de Software II



Steev Klimaszewski
Steev

Engenheiro de Sistemas Embarcados



GNU, Linux e Debian



GNU

Projeto de software livre criado por Richard Stallman em 1983.



Linux

O kernel: administra processos, memória e rede.



Distribuição

Kernel + pacotes + interface. Debian, Kali e Parrot usam o mesmo kernel.



Debian

Base do Parrot. Traz o formato .deb e as ferramentas APT/dpkg.

Quatro finalidades

Uma plataforma integrada de segurança, privacidade e desenvolvimento.

1

Segurança ofensiva

Testes autorizados de vulnerabilidades

2

Forense digital

Investigação preservando evidências

3

Engenharia reversa

Estudo de programas e binários

4

Privacidade e dev

Uso diário com foco em segurança

Pentest e forense

1 Pentest

Simula ataques para achar falhas antes de serem exploradas, não é "invadir por invadir".

FLUXO

1. Escopo e autorização
2. Coleta de informações
3. Análise de vulnerabilidades
4. Validação e relatório

2 Forense digital

Coleta e análise de evidências digitais, preservando sempre a integridade do material original.

PROCESSO

1. Preservar o dispositivo
2. Criar cópia forense
3. Calcular hash
4. Analisar e documentar

Engenharia reversa e dev

3 Engenharia reversa

Estudar um programa sem ter o código-fonte — útil para entender malware e vulnerabilidades.

Estática

Analisa o arquivo sem executá-lo.

Dinâmica

Executa e observa em ambiente controlado.

4 Privacidade e dev

Ambiente completo para programar no dia a dia: linguagens, editores e hardening.

O mesmo sistema serve para analisar e para desenvolver scripts e relatórios.

O Parrot em camadas

Segurança

AppArmor, sandboxing, hardening

Ferramentas

Pentest, forense, dev, utilitários

Sistema

Kernel Linux, serviços, KDE Plasma

Base Debian

Pacotes .deb, APT/dpkg, repositórios

da base
ao uso

Pacotes e atualizações

O Parrot usa pacotes .deb e o APT. O APT resolve dependências e instala; o dpkg opera em nível mais baixo.

COMANDOS BÁSICOS

```
apt search <nome>
sudo apt install <pacote>
sudo apt update
sudo parrot-upgrade
```

METAPACOTES

Uma lista de dependências: instala um conjunto inteiro de outros pacotes de uma vez.

Security Edition traz o parrot-tools-full pronto; a Home Edition não.

*Repositórios seguem o Debian estável;
ferramentas de segurança recebem atualizações
contínuas.*

Edições e execução

Edição	Objetivo
Security	Pentest, forense e engenharia reversa
Home	Uso diário e desenvolvimento
HTB	CTFs e Hack The Box
Raspberry Pi / IoT	ARM e dispositivos embarcados
Docker / WSL / Vagrant	Ambientes reproduzíveis

Live USB para testar; máquina virtual para estudar com segurança.

SEGURANÇA

Reduzindo a superfície de ataque

APPARMOR

enforce

Bloqueia ações não permitidas

complain

Só registra as violações

unconfined

Sem restrição de perfil

SANDBOXING

Executa programas em ambiente restrito, limitando o que enxergam ou modificam.

Menor privilégio: cada um recebe só o necessário.

REDE E VERIFICAÇÃO

Serviços de rede vêm desativados por padrão.

Hashes e assinaturas GPG verificam imagens e pacotes.

Ferramentas de segurança

A Security Edition reúne mais de 800 ferramentas — organizadas por categoria.

Categoria	Exemplo	Uso
Rede	Nmap	Mapear hosts e portas
Tráfego	Wireshark	Capturar pacotes
Web	Burp Suite	Testar aplicações
Exploração	Metasploit	Validar vulnerabilidades
Senhas	John the Ripper	Auditar hashes
Reversa	Ghidra	Decompilar binários

Quem usa o ParrotOS

- **Pentester**

Avaliações autorizadas

- **Red Team**

Simulações de ataque

- **Analista**

Investiga vulnerabilidades

- **Forense**

Discos, logs e evidências

- **Pesquisador**

Estuda malware

- **Estudante**

CTFs e Hack The Box

- **Desenvolvedor**

Scripts e utilitários

Parrot x Kali x BlackArch

Critério	Parrot	Kali	BlackArch
Base	Debian	Debian	Arch
Foco	Segurança + dev	Pentest	Pesquisa
Ferramentas	800+	Centenas	2.800+
Pacotes	APT / dpkg	APT / dpkg	pacman
Curva	Média	Média	Alta

Mesmo nicho, prioridades diferentes: Kali é a referência em pentest; BlackArch tem o maior repositório; o Parrot soma segurança e uso diário.

Vantagens e limitações

PONTOS FORTES

- Base Debian madura
- Arsenal amplo e atualizado
- Security ou Home, à escolha
- Hardening e AppArmor
- Roda em VM, USB, Docker e mais

LIMITAÇÕES

- Arsenal não substitui conhecimento
- Complexidade e armazenamento
- Uso indevido tem risco legal
- Drivers extras para Wi-Fi/GPU
- Uso simples pode preferir outra distro

Curiosidades

Builds otimizados

Pacotes para CPUs modernas, ganhos em criptografia e hashing.

RISC-V

Suporte a essa arquitetura aberta desde o Parrot 7.

Arsenal Explorer

Site (2026) para navegar pelo catálogo de ferramentas.

O nome “Parrot”

Referência bem-humorada ao papagaio dos piratas.

Conclusão

“ParrotOS é uma distribuição completa que une base Debian, políticas de segurança e um arsenal especializado em um laboratório portátil de cibersegurança.”

- Debian fornece a base; o kernel administra os recursos
- KDE e APT formam a experiência de uso
- AppArmor restringe riscos de segurança
- A melhor escolha depende do objetivo do usuário

REFERÊNCIAS

<https://docs.parrotsec.org/blog/2026-04-23-parrot-arsenal-explorer>

<https://docs.parrotsec.org/how-it-works/>

<https://blackarch.org/>

<https://www.kali.org/docs/introduction/what-is-kali-linux/>

<https://pt.console-linux.com/?p=2689>

<https://www.instagram.com/palinuro.me/>