

# Gnu/Linux

# Kali Linux

Workshop – Projeto Connor



# Programação

01

## História

História - Distribuição

02

## Instalação

Instalação do Kali Linux

03

## Softwares

Netcat, Nmap, Hydra, Nikto, John The Ripper, Gobuster, Aircrack-ng

04

## Tipos Pentest

Black Box, Gray Box, White Box

05

## Fases Pentest

Planning, Scanning, Exploitation, Post Exploitation, Maintaining Access, Reporting

06

## Tipos de Ataque

Brute Force, Command Injection, SQL Injection, XSS, JavaScript

# Programação

07

## Certificações

CEH, OSCP, EJPT, SECURITY +,  
ISC<sup>2</sup>

08

## CTF's

Capture the Flag -  
Challenges

09

## Let's Hack

Startup, Mr.Robot

10

## Quiz

Kahoot

11

## Hands On

PickleRick - Tryhackme



01

# História

Kali Linux





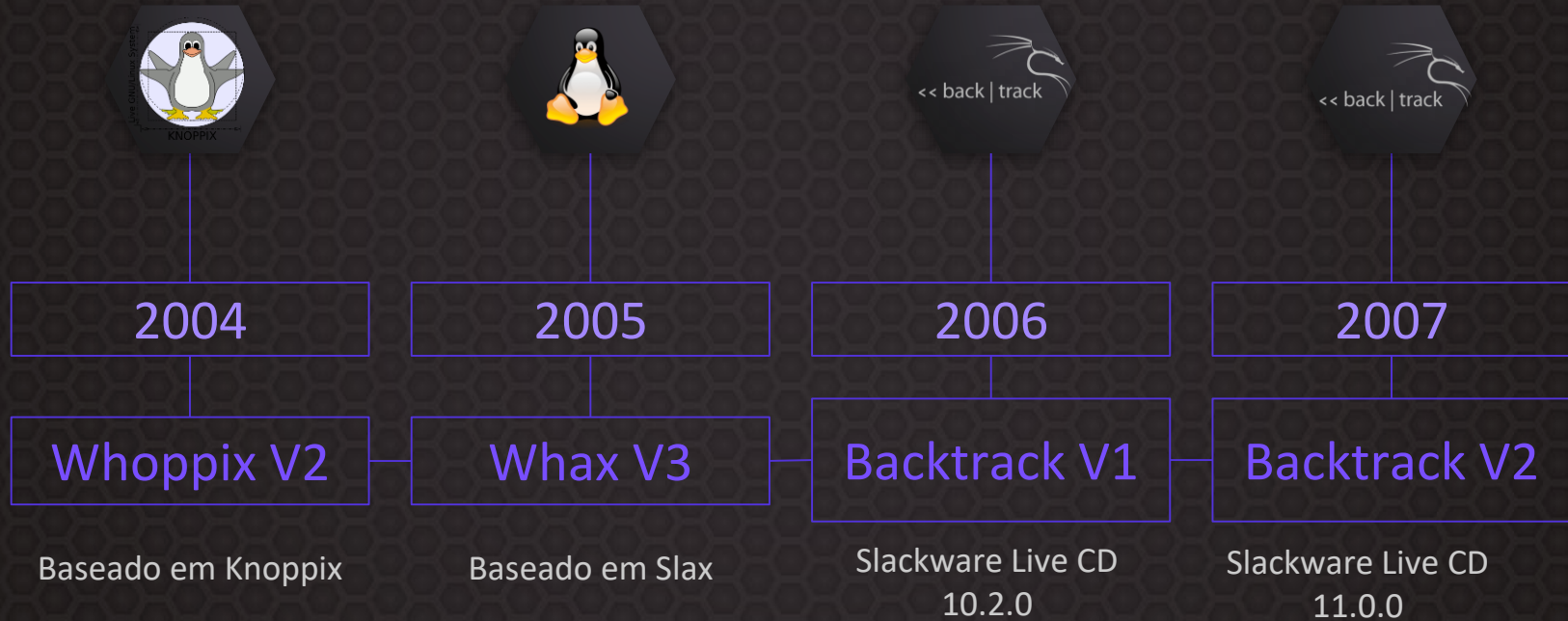
<< back | track



debian



# Kali Linux



# Kali Linux





# Kali Linux



2015

Kali Linux V2

Baseado em Debian 8



2016

Kali Linux  
Rolling

Baseado em Debian  
Testing



2019

Kali Linux  
v2019.4

Interface Default  
Gnome -> Xfce



2020

Kali Linux  
v2020.3

Shell Default  
Bash -> Zsh



# User Interface



# Penetration Test



# Forense







**OFFENSIVE<sup>®</sup>**  
security





02

# Instalação

Kali Linux



Kali.org





KALI

[GET KALI](#) [BLOG](#) [DOCUMENTATION](#) [COMMUNITY](#) [COURSES](#) [DEVELOPERS](#) [ABOUT](#)




## The most advanced Penetration Testing Distribution

Kali Linux is an open-source, Debian-based Linux distribution geared towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering.

[DOWNLOAD](#) 


[DOCUMENTATION](#) 

[DOWNLOAD](#) 

[DOCUMENTATION](#) 

## Choose **your** Kali

LIGHT ☒ DARK



**ARM**

- ✓ Range of hardware from the humblest devices and to high-end modern servers
- ✓ System architecture limits certain packages
- ✗ Not always customized kernel

Works on relatively inexpensive & low powered Single Board Computers (SBCs) as well as modern ARM based laptops, which combine high speed with long battery life.



**Installer Images**

- ✓ Direct access to hardware
- ✓ Customized Kali kernel
- ✓ No overhead

Single or multiple boot KVM, giving you complete control over the hardware access (perfect for in-built Wi-Fi and GPU), enabling the best performance.

 Recommended




**Virtual Machines**

- ✓ Snapshot functionality
- ✓ Isolated environment
- ✓ Customized Kali kernel
- ✗ Limited direct access to hardware
- ✗ Higher system requirements

VMware & VirtualBox pre-built images. Allowing for a Kali install without altering the host OS with additional features such as snapshots. Vagrant images for quick spin-up also available.

 Recommended



**Mobile**

- ✓ Kali Linux on Android
- ✓ Kali in your pocket, on the go
- ✓ Mobile version face compact view


A mobile penetration testing platform for Android devices, based on Kali Linux, Kali NetHunter consists of an NetHunter App, App Store, Kali Container, and KaliX.



**Cloud**

- ✓ Fast deployment
- ✓ Can leverage provider's resources
- ✗ Provider may become costly
- ✗ Not always customized kernel


Hosting providers which have Kali Linux pre-installed, ready to go, without worrying about infrastructure maintenance.



**Containers**

- ✓ Low overhead to access Kali install
- ✗ Overhead actions only
- ✗ Not Kali customized kernel
- ✗ No direct access to hardware


Using Docker or LXD, allows for extremely quick and easy access to Kali's tool set without the overhead of an isolated virtual machine.



**Live Boot**

- ✓ On-stand host system
- ✓ Direct access to hardware
- ✓ Customized Kali kernel
- ✗ Performance decrease when heavy I/O

Quick and easy access to a full Kali install. Your Kali, always with you, without altering the host OS, plus allows you to benefit from hardware access.



**WSL**

- ✓ Access to the Kali install through the WSL framework
- ✗ Overhead actions only
- ✗ Not Kali customized kernel
- ✗ No direct access to hardware

Windows Subsystem for Linux (WSL) is included out of the box with modern Windows. Use Kali (and Win-Kali) without installing additional software.



03

# Softwares

Kali Linux

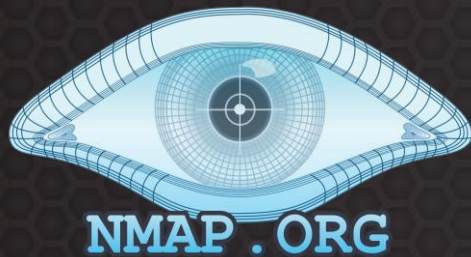






- Canivete suíço
- Port Scanning
- Encaminhamento de Porta
- Transferência de Arquivos
- Chat
- Shell Reverso





- Enumeração de Serviços
- Port Scanning
- Host Discovery
- Versões sistemas e serviços





- Brute Force
- Interface Gráfica
- Dicionário
- Não dicionário
- SSH
- Telnet
- FTP
- Módulos Extras

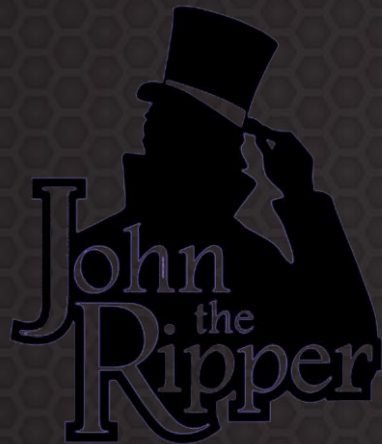






- Perl
- Web Scanner
- Vulnerabilidades





- Brute Force
- Padrões DES, MD4 e MD5



# GOBUSTER

- Bruteforce
- Enumeração de diretório
- Enumeração de DNS
- Enumeração s3 (AWS)







- Gerador de Wordlists
- Charset incluso
- Padrões conhecidos





- Wireless Attack
- Bruteforce





04

# Tipos PenTest





## Tipos de Pentest



Black Box



Gray Box



White Box





Black Box

- Sem informações
- Pentest externo
- Fundamental um bom scanning
- Tempo elevado para ser completo





Gray Box

- Informações parciais
- Custo benefício







## White Box

- Informações prévias
- Relatórios mais completos
- Maior eficiência quando comparado aos outros tipos
- Maior custo financeiro quando comparado aos outros tipos





05

# Fases Pentest





# Planning





# Planning

- Contrato
- Non disclosure agreement
- Engenharia Social
- Definição do escopo





Scanning



Footprint



FingerPrint





# Footprint



- Whois
- Archive.org
- Sites de empregos
- Google Hacking



# FingerPrint



- NMAP
- Gobuster
- Nikto



HA HA HA



Exploitation





## Ganho de acesso

- Reverse Shell
- Password
- Bruteforce



HA HA HA



# Post Exploitation



## Ganho de acesso privilegiado (Root)

- Privilege Escalation
- Reverse Shell
- Password
- Bruteforce
- Exploit







# Maintaining Access



## Mantendo acesso

- Malware
- Keylogger
- Backdoor





# Reporting





Sumário Executivo



Relatório Técnico



## Sumário Executivo



- Resumo
- Não técnico
- Infográficos
- Previsão de tempo de resolução.



## Relatório Técnico



- Vulnerabilidades encontradas
- Explicação de como executá-las
- Soluções para as vulnerabilidades







06

# Tipos de Ataques





- Aplicação Web Vulnerável
- Treino Pentesting
- Níveis de dificuldade



# Brute Force



10000000	abcdefg0	root
10000001	abbcdefe	admin
10000002	z91840ds	Password
89999999	445654#@!	qwerty
99999999	zzzzzzzz	a1s2d3f4

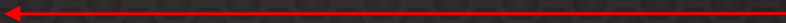




# Command Injection



google.com ; ls



Help  
Index.php  
source



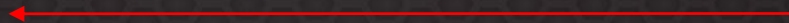
# File Upload



# SQL Injection



' or '1=1' #



Admin  
Gordon  
Hack  
Pablo  
Bob





# Javascript



Console.log

Source Code





07

# Certificações

Kali Linux









08

CTF's

Kali Linux



## Capture the Flag (CTF'S)

- Ambientes Controlados
- Desafios
- Temas específicos
- Exploração





Try  
Hack  
Me



Capture  
The Flag



Pwn2Win  
CTF



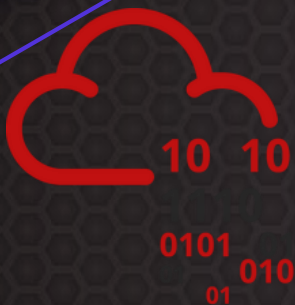




09

Let's Hack





Try  
Hack  
Me





10

Quiz





**QUIZ!**

**Kahoot!**





11

# Hands On

Let's do it yourself






Try  
Hack  
Me








“O verdadeiro hacker não se autodenomina  
com este título, ele é denominado.”

Hacker anônimo





# Obrigado!

Tem alguma dúvida?

renan.souza@facens.br  
lucca.campos@facens.br  
Projeto Connor