

Penetration Testing com Kali Linux



Palestrante: Fernando Santorsula

www.fhs.pro.br





Introdução ao penetration testing

Penetration testing (teste de penetração) nada mais é que um método legal e autorizado pelo contratante ou empresa, que permite que o pentester ou hacker ético testar as fraquezas de sistemas computacionais.



www.kali.org





Introdução ao penetration testing

Durante os testes realizados com o **Kali Linux**, ataques são executados ao sistema que for permitido efetuar os mesmos, caso seja bem sucedido, são apresentadas as chamadas “Provas de Conceito”, em inglês **Proof of Concept - POC**)



www.kali.org





Introdução ao penetration testing

Penetration testing **NÃO** deve ser confundido com:

“Análise de vulnerabilidade”, pois analisar e encontrar vulnerabilidade é outra técnica da Segurança da Informação.



www.kali.org





Tipos de penetration testing

Existem muitos tipos de penetration testing e que podemos fazer com o Kali Linux, iremos abordar dois tipos:

White Box e Black Box



www.kali.org





Tipos de penetration testing

White Box ou caixa branca é o hacker ético que tem total conhecimento do ambiente a ser explorado, entre eles:

Redes de Computadores, Sistemas Operacionais e afins...



www.kali.org



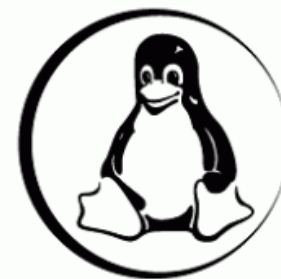


Tipos de penetration testing

Black Box ou caixa preta é o pentester que não possui um conhecimento prévio do ambiente a ser realizados os testes em redes ou softwares.



www.kali.org





Tipos de penetration testing

Qual tipo de teste é mais adequado ?





Tipos de penetration testing

Nenhum! A boa prática é efetuar uma análise do cenário onde decisões serão tomadas para o penetration testing ser realizado.



www.kali.org





Escopo do penetration testing

- * Modalidade dos testes: black box ou white box
- * Quais serviços / equipamentos ficaram fora
- * Requisitos operacionais
- * Recursos
- * Infraestrutura
- * Sistemas
- * Serviços
- * Máquinas
- * Pessoas envolvidas
- * Impactos / Interrupções de serviços
- * Período a ser aplicado
- * Tempo de parada



www.kali.org



Segurança da Informação

Não podemos esquecer dos pilares da Segurança da Informação antes de qualquer penetration testing

Confiabilidade, Integridade e Disponibilidade

E temos que ter ciência que NÃO existe segurança computacional **100%** segura



www.kali.org





Sobre o Kali Linux

É uma poderosa ferramenta baseada no sistema Debian, sucessor e uma reconstrução do seu antecessor: **BackTrack**, o Kali Linux possui mais de 300 ferramentas para testes de intrusão para os mais diversos penetration testing a ser feito...

Obs. A última versão possui suporte a plataforma ARM



www.kali.org





Instalação do Kali Linux

Pré-requisitos para instalação:

No mínimo 8 GB de espaço em disco para a instalação.

No mínimo 512MB de RAM para as arquiteturas i386 e amd64.

Suporte a boot pelo drive de CD-DVD / USB

Suporte a instalações via VirtuaBox / Wmware Player

Tamanho da imagem .ISO – 2.6GB

Plataformas: 32 e 64 bits



www.kali.org





Tipos de instalação do Kali Linux





Instalação do Kali Linux

The image shows the Kali Linux installation language selection screen. At the top, there is a banner with the Kali Linux logo and the tagline "THE QUIETER YOU BECOME, THE MORE YOU ARE ABLE TO HEAR." Below the banner, the text "Select a language" is displayed. A message states: "Choose the language to be used for the installation process. The selected language will also be the default language for the installed system." Below this, the word "Language:" is followed by a list of languages. The "English" option is highlighted in red. At the bottom, there are three buttons: "Screenshot", "Go Back", and "Continue".

Select a language

Choose the language to be used for the installation process. The selected language will also be the default language for the installed system.

Language:

Chinese (Simplified)	-	中文(简体)
Chinese (Traditional)	-	中文(繁體)
Croatian	-	Hrvatski
Czech	-	Čeština
Danish	-	Dansk
Dutch	-	Nederlands
Dzongkha	-	ཇོངཀ་མ་གསལ་སྐད་
English	-	English
Esperanto	-	Esperanto
Estonian	-	Eesti
Finnish	-	Suomi
French	-	Français
Galician	-	Galego
Georgian	-	ქართული
German	-	Deutsch
Greek	-	Ελληνικά

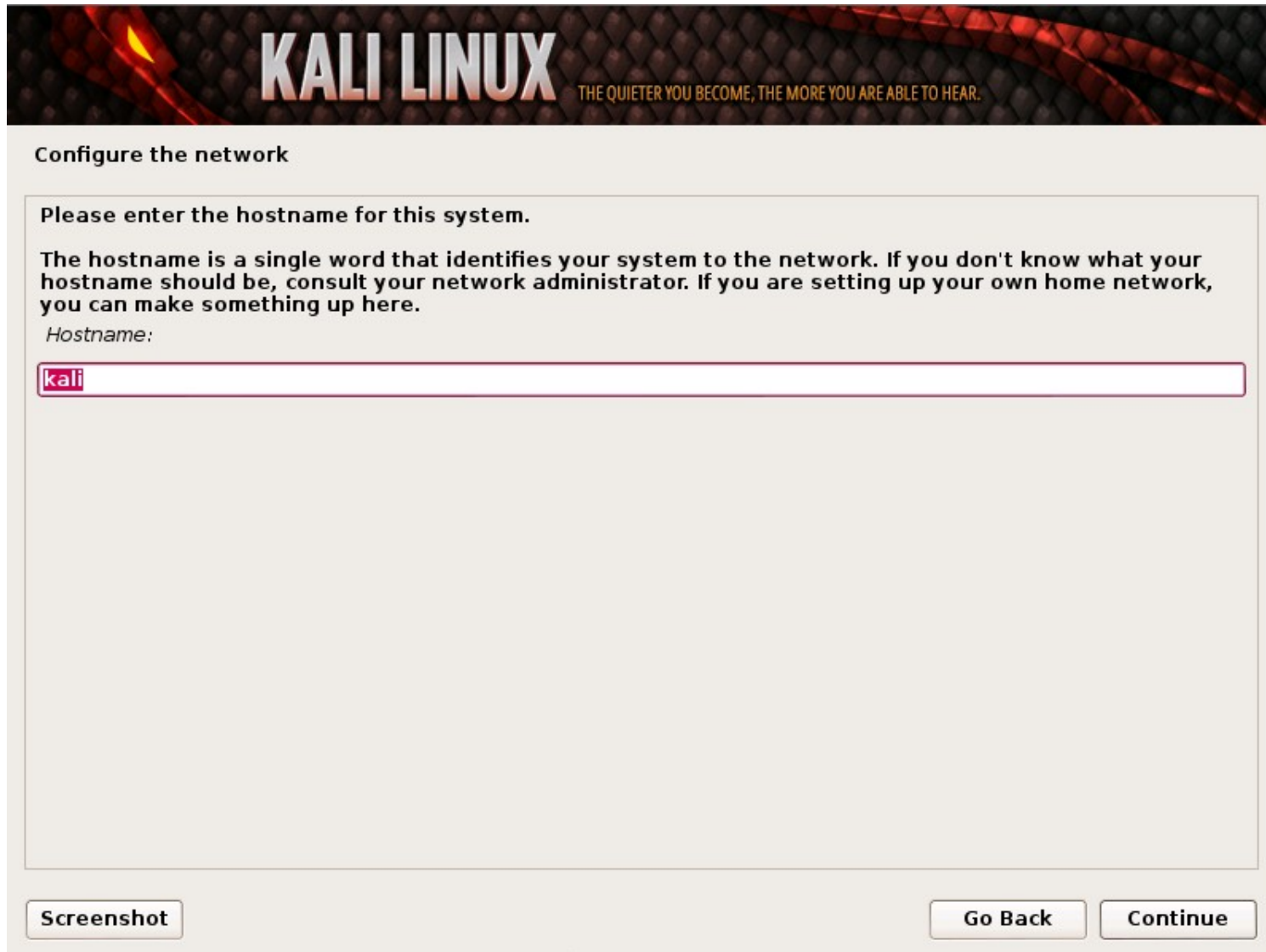
Screenshot

Go Back

Continue



Instalação do Kali Linux



KALI LINUX THE QUIETER YOU BECOME, THE MORE YOU ARE ABLE TO HEAR.

Configure the network

Please enter the hostname for this system.

The hostname is a single word that identifies your system to the network. If you don't know what your hostname should be, consult your network administrator. If you are setting up your own home network, you can make something up here.

Hostname:

Screenshot

Go Back Continue



Instalação do Kali Linux

Set up users and passwords

You need to set a password for 'root', the system administrative account. A malicious or unqualified user with root access can have disastrous results, so you should take care to choose a root password that is not easy to guess. It should not be a word found in dictionaries, or a word that could be easily associated with you.

A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.

The root user should not have an empty password. If you leave this empty, the root account will be disabled and the system's initial user account will be given the power to become root using the "sudo" command.

Note that you will not be able to see the password as you type it.

Root password:

Please enter the same root password again to verify that you have typed it correctly.

Re-enter password to verify:

Screenshot

Go Back

Continue



Instalação do Kali Linux

KALI LINUX THE QUIETER YOU BECOME, THE MORE YOU ARE ABLE TO HEAR.

Configure the clock

If the desired time zone is not listed, then please go back to the step "Choose language" and select a country that uses the desired time zone (the country where you live or are located).

Select your time zone:

- Eastern**
- Central
- Mountain
- Pacific
- Alaska
- Hawaii
- Arizona
- East Indiana
- Samoa

Screenshot Go Back Continue




Instalação do Kali Linux





Instalação do Kali Linux



Partition disks

If you continue, the changes listed below will be written to the disks. Otherwise, you will be able to make further changes manually.

WARNING: This will destroy all data on any partitions you have removed as well as on the partitions that are going to be formatted.

The partition tables of the following devices are changed:
SCSI3 (0,0,0) (sda)

The following partitions are going to be formatted:
partition #1 of SCSI3 (0,0,0) (sda) as ext4
partition #5 of SCSI3 (0,0,0) (sda) as swap

Write the changes to disks?

☐ No

☒ Yes



Instalação do Kali Linux

OBSERVAÇÃO! Se você selecionar “NÃO” nesta tela, você **NÃO** será capaz de instalar pacotes dos repositórios do Kali.

www.kali.org





Instalação do Kali Linux

KALI LINUX THE QUIETER YOU BECOME, THE MORE YOU ARE ABLE TO HEAR.

Configure the package manager

A network mirror can be used to supplement the software that is included on the CD-ROM. This may also make newer versions of software available.

Use a network mirror?

☐ No

☒ Yes

Screenshot

Go Back Continue



Instalação do Kali Linux

KALI LINUX THE QUIETER YOU BECOME, THE MORE YOU ARE ABLE TO HEAR.

Install the GRUB boot loader on a hard disk

It seems that this new installation is the only operating system on this computer. If so, it should be safe to install the GRUB boot loader to the master boot record of your first hard drive.

Warning: If the installer failed to detect another operating system that is present on your computer, modifying the master boot record will make that operating system temporarily unbootable, though GRUB can be manually configured later to boot it.

Install the GRUB boot loader to the master boot record?

☐ No

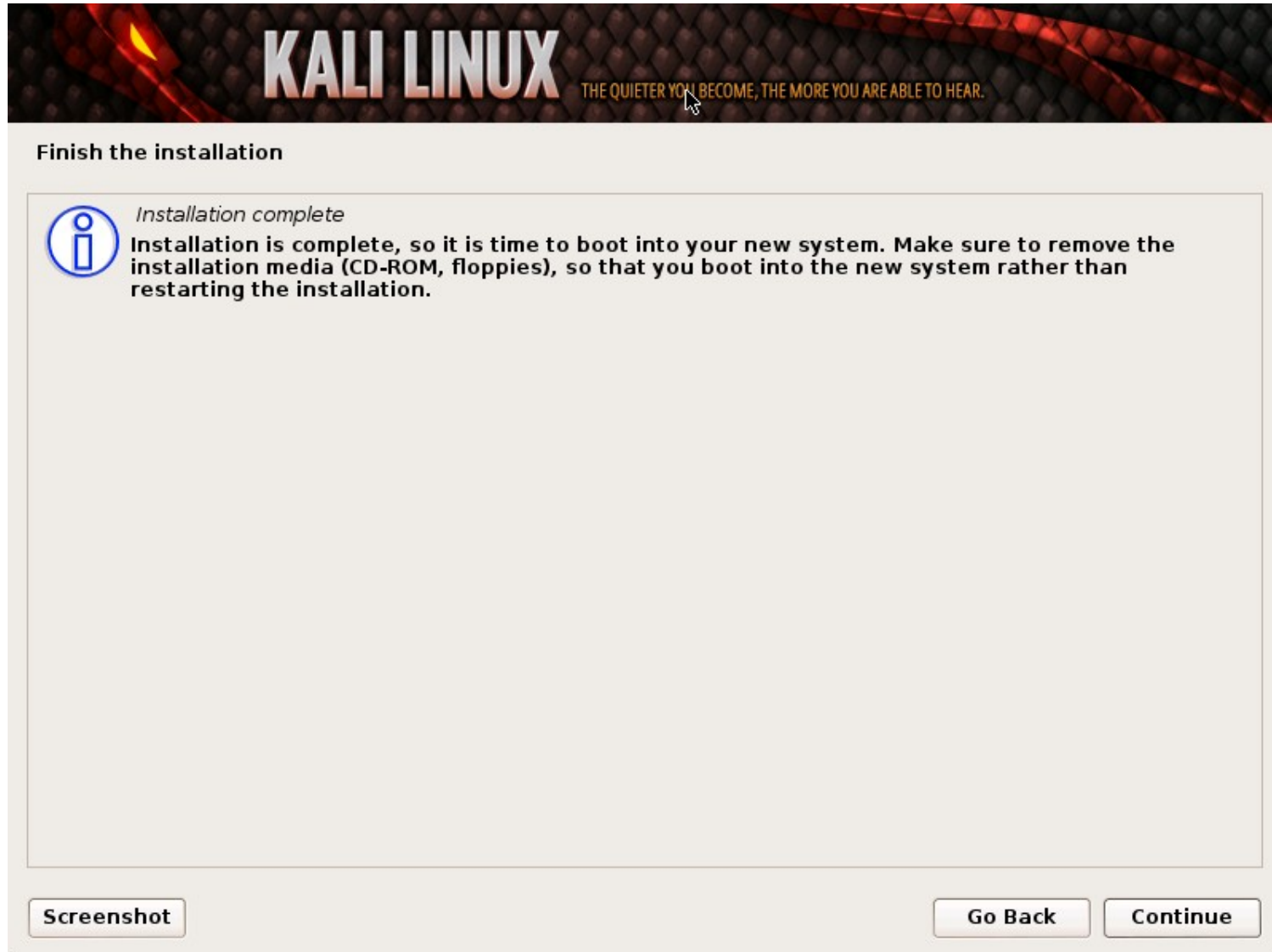
☒ Yes

Screenshot

Go Back Continue



Instalação do Kali Linux





Ferramentas do Kali Linux

Análise de DNS



- 🔍 [dnsdict6](#)
- 🔍 [dnsenum](#)
- 🔍 [dnsmap](#)
- 🔍 [dnsrecon](#)
- 🔍 [dnsrevenue6](#)
- 🔍 [dnstracer](#)
- 🔍 [dnswalk](#)
- 🔍 [fierce](#)
- 🔍 [maltego](#)
- 🔍 [nmap](#)
- 🔍 [urlcrazy](#)
- 🔍 [zenmap](#)

www.kali.org



Ferramentas do Kali Linux

IDS (Intrusion Detection System)

IPS (Intrusion Prevention System)



 fragroute

 fragrouter

 ftest

 lbd

 wafw00f

www.kali.org



Ferramentas do Kali Linux

Identificação de hosts



- alive6
- arping
- cdpsnarf
- detect-new-ip6
- detect_sniffer6
- dmitry
- dnmap-client
- dnmap-server
- fping
- hping3
- inverse_lookup6
- miranda
- ncat
- netdiscover
- nmap
- passive_discovery6
- thcping6
- wol-e
- xprobe2
- zenmap

www.kali.org



Ferramentas do Kali Linux

Network Scanners



🔍 dmitry

🔍 dnmap-client

🔍 dnmap-server

🔍 netdiscover

🔍 nmap

🔍 zenmap

www.kali.org



Ferramentas do Kali Linux

Route Analysis



- 🔍 otrace
- 🔍 dnmap-client
- 🔍 dnmap-server
- 🔍 intrace
- 🔍 netmask
- 🔍 trace6

www.kali.org



Ferramentas do Kali Linux

SMB Analysis



🔍 acccheck

🔍 nbtscan

🔍 nmap

🔍 zenmap

www.kali.org



Ferramentas do Kali Linux

SMTP Analysis



🔍 nmap

🔍 smtp-user-enum

🔍 swaks

🔍 zenmap

www.kali.org



Ferramentas do Kali Linux

SNMP Analysis



🔍 braa

🔍 cisco-auditing-tool

🔍 cisco-torch

🔍 copy-router-config

🔍 merge-router-config

🔍 nmap

🔍 onesixtyone

🔍 snmpcheck

🔍 zenmap

www.kali.org



Ferramentas do Kali Linux

SSL Analysis



🔍 sslcaudit

🔍 ssldump

🔍 sslh

🔍 sslscan

🔍 sslsniff

🔍 sslsplit

🔍 sslstrip

🔍 sslyze

🔍 stunnel4

🔍 tlssled

www.kali.org



Ferramentas do Kali Linux

Telephony Analysis



www.kali.org



Ferramentas do Kali Linux

Traffic Analysis



- 🔍 Otrace
- 🔍 cdp snarf
- 🔍 ftest
- 🔍 intrace
- 🔍 irpas-ass
- 🔍 irpass-cdp
- 🔍 p0f
- 🔍 tcpflow
- 🔍 wireshark



www.kali.org



Ferramentas do Kali Linux

VoIP Analysis



 ace

 enumiax

www.kali.org



Ferramentas do Kali Linux

VPN Analysis



 ike-scan

www.kali.org



SGBD



Ferramentas do Kali Linux

- bbqsql
- dbpwaudict
- hexorbase
- jsql
- mdb-export
- mdb-hexdump
- mdb-parsecsv
- mdb-sql
- mdb-tables
- oscanner
- sidguesser
- sqldict
- sqlmap
- sqlninja
- sqlsus
- tnscmd10g

www.kali.org



Ferramentas do Kali Linux

Scanners



 lynis

 nikto

 nmap

 unix-privesc-check

 zenmap






www.kali.org



Ferramentas do Kali Linux

OpenVAS (Open Vulnerability Assessment System (Sistema Aberto de Avaliação de Vulnerabilidade))



-  `openvas check setup`
-  `openvas feed update`
-  `openvas initial setup`
-  `openvas start`
-  `openvas stop`

www.kali.org



Ferramentas do Kali Linux

Web Applications



CMS Identification



blindelephant



plecost



wpscan

www.kali.org




Ferramentas do Kali Linux

Web Applications Proxies




 burpsuite

 owasp-zap

 paros

 proxystrike

 vega

 webscarab


www.kali.org




Ferramentas do Kali Linux

Web Crawlers (Rastreadores Web)




 apache-users


 burpsuite

 cutycapt

 dirb

 dirbuster

 owasp-zap

 recon-ng

 vega

 webscarab

 webslayer

www.kali.org



Ferramentas do Kali Linux

Web Vulnerability Scanners



⚙️ arachni_web

⚙️ burpsuite

⚙️ cadaver

⚙️ davtest

⚙️ deblaze

⚙️ fimap

⚙️ grabber

⚙️ joomscan

⚙️ jsql

⚙️ nikto

⚙️ owasp-zap

⚙️ padbuster

⚙️ proxystrike

⚙️ skipfish

⚙️ sqlmap

⚙️ uniscan-gui

⚙️ vega

⚙️ w3af

⚙️ wapiti

⚙️ webscarab

⚙️ webshag-gui

⚙️ websploit

⚙️ whatweb

⚙️ wpscan

⚙️ xsser

www.kali.org



Ferramentas do Kali Linux

Password Attacks (Offline)



cachedump

chntpw

cmospwd

crunch

cudahashcat-plus

dictstat

fcrackzip

hashcat

hash-identifier

john

johnny

lsadump

www.kali.org



Ferramentas do Kali Linux

Password Attacks (Online)



acccheck

burpsuite

cewl

cisco-auditing-tool

dbpwaudict

findmyhash

hydra

hydra-gtk

keimpx

medusa

ncrack

onesistyone








www.kali.org



Ferramentas do Kali Linux

Bluetooth Tools



-  bluelog
-  bluemaho
-  blueranger
-  bluesnarfer
-  btscanner
-  fang
-  spooftooth

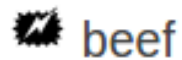
www.kali.org



Ferramentas do Kali Linux

Exploitation Tools

BeEf XSS Framework



www.kali.org



Ferramentas do Kali Linux

Cisco Attacks



- ✚ cisco-auditing-tool
- ✚ cisco-global-exploiter
- ✚ cisco-ocs
- ✚ cisco-torch
- ✚ yersinia

www.kali.org



Ferramentas do Kali Linux

Metasploit (Análise de vulnerabilidades)



- ✦ metasploit community / pro
- ✦ metasploit diagnostic logs
- ✦ metasploit diagnostic shell
- ✦ metasploit framework
- ✦ update metasploit

www.kali.org



Ferramentas do Kali Linux

Network Exploitation



⚡ armitrage

⚡ exploit6

⚡ ikat

⚡ jboss-autopwn-linux

⚡ jboss-autopwn-win

⚡ termineter

www.kali.org



Ferramentas do Kali Linux


Sniffing (Interceptar e registrar tráfego)
Spoofing (Mascarar pacotes IP)



www.kali.org

 darkstat

 dnscchef


 dnsspoof

 dnsiff


 ettercap-graphical

 hexinject


 mailsnarf

 msgsnarf

 netsniff-ng

 passive_discovery6

 responder

 sslsniff

 tcpflow

 urlsnarf

 webmitm



Ferramentas do Kali Linux


Hardware Hacking

Android Tools



 apktool

 baksmali

 dex2jar

 smali

www.kali.org

Obs. se quiser conhecer todas as ferramentas do Kali Linux, acesse:

<http://tools.kali.org/tools-listing>



Dúvidas





Sobre o palestrante

Atua a mais de 10 anos na área de Informática no segmento de Redes de Computadores, Servidores Linux, Segurança da Informação, Consultoria e Projetos em Redes LAN / WAN, Consultoria e Projetos de CFTV e Desenvolvimento Web com CMS: WordPress e Joomla. Atualmente trabalha na empresa inglesa **British Telecom** como Analista de TI e também trabalha como professor universitário na **ESAMC** (Escola Superior de Administração, Marketing e Comunicação), Campus – Sorocaba/SP. O Prof. Fernando Santorsula é graduado em Redes de Computadores pela (UNIP) Universidade Paulista (Campus – Sorocaba/SP), Pós-graduado em Redes de Computadores pela (UNIMEP) Universidade Metodista de Piracicaba/SP.





Contatos do palestrante

E-mails:

fernando.gnu@gmail.com

fernando@fhs.pro.br

Site Oficial:

www.fhs.pro.br

Download da Palestra:

www.fhs.pro.br/flisol-2016



INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
SÃO PAULO | CAMPUS SALTO

Obrigado !

E até o



de 2017

ATENÇÃO! Não vá embora! Aguarde a foto!!!



Palestra: Penetration Testing com Kali Linux

Palestrante:

Fernando Henrique Santorsula
fernando.gnu@gmail.com