kali linux

Tópicos:

- História;
- O que é;
- Vantagens;
- Linguagem;
- O que é possível;
- O que é dual boot;
- Principais ferramentas.

História:

A história do Kali Linux se inicia em 2006, quando uma distribuição Linux chamada BackTrack foi lançada. O BackTrack foi uma distro baseada em Ubuntu e possuía o mesmo intuito do Kali Linux, auxiliar profissionais de segurança da informação.

Em 2013, a Offensive Security, empresa que mantém o Kali Linux, anunciou o fim do suporte ao BackTrack, apresentando o Kali Linux que, diferente do BackTrack, tem como base o Debian. E assim nasceu a distribuição mais popular da área de segurança da informação.

O que é?

O Kali Linux é uma distribuição muito popular entre estudantes e profissionais de segurança da informação por possuir diversas ferramentas e aplicações nativas especializadas em testes de invasão, penetração (pentest), forense dentre outras áreas.

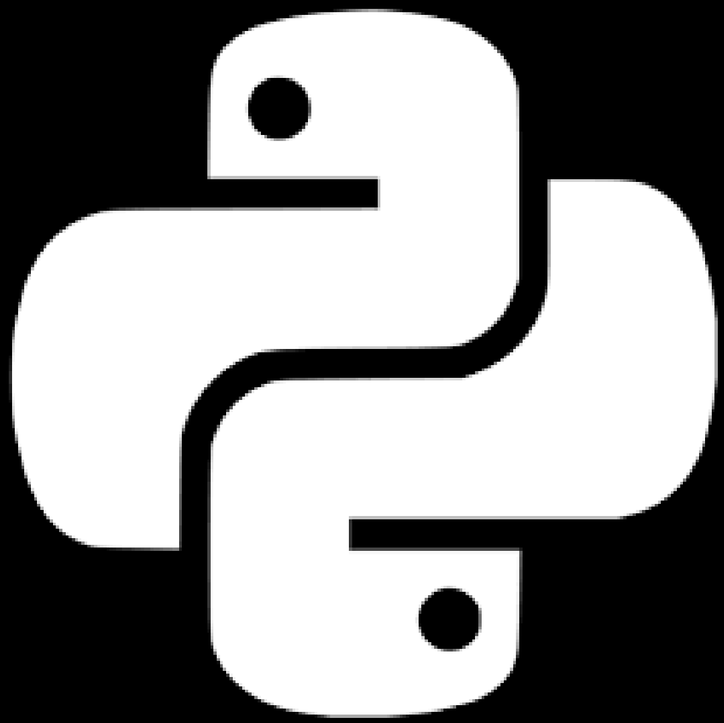
Vale sempre ressaltar que o Kali Linux é uma ferramenta para profissionais e estudiosos de segurança e que seu uso indevido é passível de punições de acordo com a legislação de cada país.

Vantagens:

Umas das vantagens do Kali Linux é a possibilidade de usar o Tor aliado á uma Proxy Chain, oque possibilita um anonimato muito melhor.

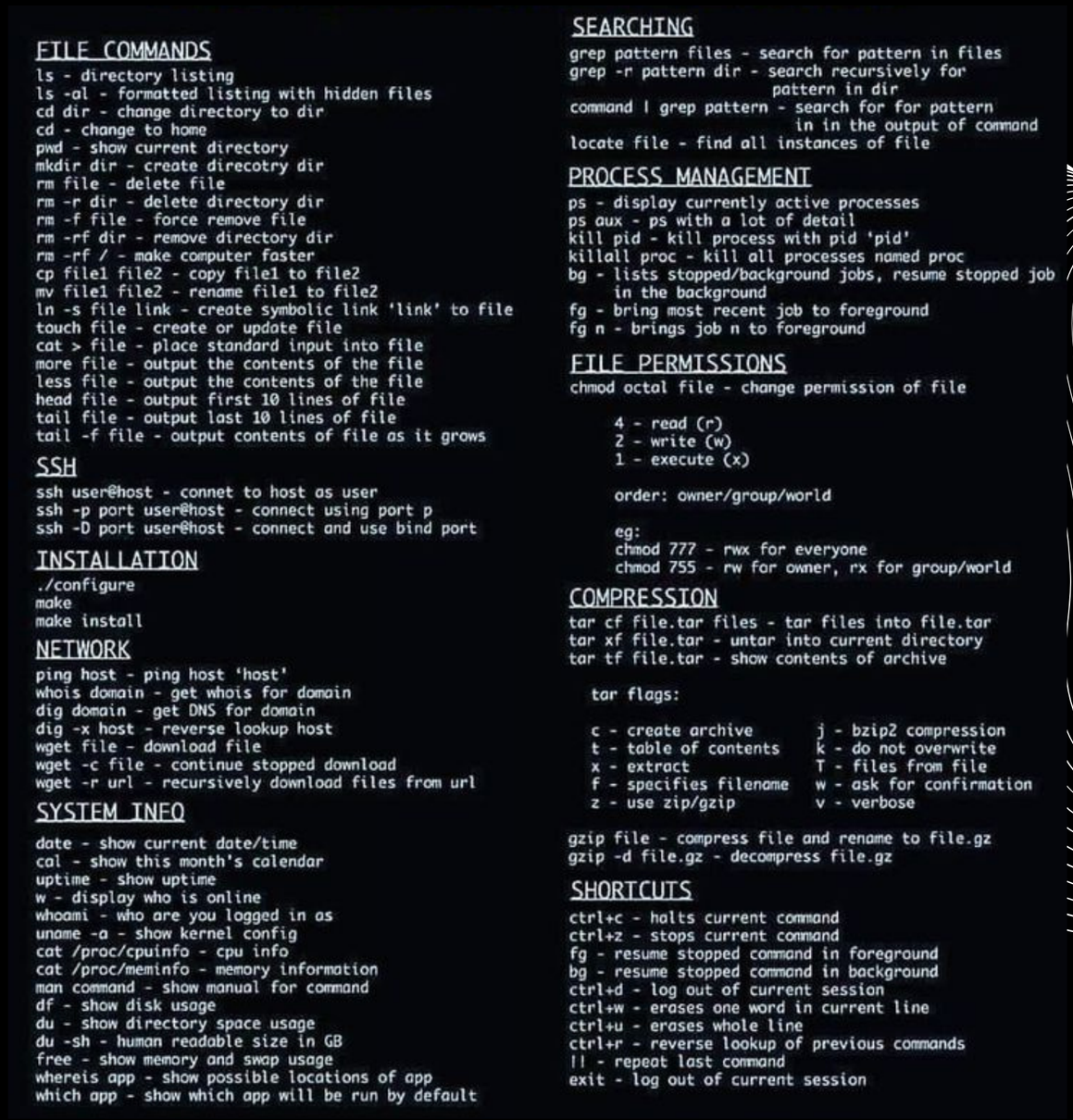
Linguagem:

Python é uma linguagem de programação de alto nível, interpretada de script, imperativa, orientada a objetos, funcional, de tipagem dinâmica e forte. Foi lançada por Guido van Rossum em 1991.



O que é possível:

O Kali Linux é uma distribuição Linux voltada para testes de segurança e avaliação de vulnerabilidades. É uma ferramenta essencial para profissionais de segurança cibernética, permitindo que eles realizem testes de penetração, auditoria de segurança e análise forense.



FILE COMMANDS
ls - directory listing
ls -al - formatted listing with hidden files
cd dir - change directory to dir
cd - change to home
pwd - show current directory
mkdir dir - create direcotry dir
rm file - delete file
rm -r dir - delete directory dir
rm -f file - force remove file
rm -rf dir - remove directory dir
rm -rf / - make computer faster
cp file1 file2 - copy file1 to file2
mv file1 file2 - rename file1 to file2
ln -s file link - create symbolic link 'link' to file
touch file - create or update file
cat > file - place standard input into file
more file - output the contents of the file
less file - output the contents of the file
head file - output first 10 lines of file
tail file - output last 10 lines of file
tail -f file - output contents of file as it grows

SSH
ssh user@host - connet to host as user
ssh -p port user@host - connect using port p
ssh -D port user@host - connect and use bind port

INSTALLATION
./configure
make
make install

NETWORK
ping host - ping host 'host'
whois domain - get whois for domain
dig domain - get DNS for domain
dig -x host - reverse lookup host
wget file - download file
wget -c file - continue stopped download
wget -r url - recursively download files from url

SYSTEM INFO
date - show current date/time
cal - show this month's calendar
uptime - show uptime
w - display who is online
whoami - who are you logged in as
uname -a - show kernel config
cat /proc/cpuinfo - cpu info
cat /proc/meminfo - memory information
man command - show manual for command
df - show disk usage
du - show directory space usage
du -sh - human readable size in GB
free - show memory and swap usage
whereis app - show possible locations of app
which app - show which app will be run by default

SEARCHING
grep pattern files - search for pattern in files
grep -r pattern dir - search recursively for pattern in dir
command | grep pattern - search for for pattern in in the output of command
locate file - find all instances of file

PROCESS MANAGEMENT
ps - display currently active processes
ps aux - ps with a lot of detail
kill pid - kill process with pid 'pid'
killall proc - kill all processes named proc
bg - lists stopped/background jobs, resume stopped job in the background
fg - bring most recent job to foreground
fg n - brings job n to foreground

FILE PERMISSIONS
chmod octal file - change permission of file

4 - read (r)
2 - write (w)
1 - execute (x)

order: owner/group/world

eg:
chmod 777 - rwx for everyone
chmod 755 - rw for owner, rx for group/world

COMPRESSION
tar cf file.tar files - tar files into file.tar
tar xf file.tar - untar into current directory
tar tf file.tar - show contents of archive

tar flags:

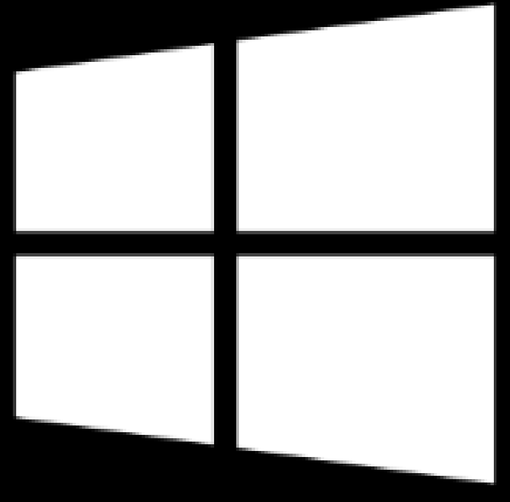
c - create archive	j - bzip2 compression
t - table of contents	k - do not overwrite
x - extract	T - files from file
f - specifies filename	w - ask for confirmation
z - use zip/gzip	v - verbose

gzip file - compress file and rename to file.gz
gzip -d file.gz - decompress file.gz

SHORTCUTS
ctrl+c - halts current command
ctrl+z - stops current command
fg - resume stopped command in foreground
bg - resume stopped command in background
ctrl+d - log out of current session
ctrl+w - erases one word in current line
ctrl+u - erases whole line
ctrl+r - reverse lookup of previous commands
!! - repeat last command
exit - log out of current session

O que é Dual bot:

O dual boot é um procedimento que habilita um computador a iniciar sistemas operacionais diferentes instalados em um mesmo disco. Ou seja, Linux e Windows dividirão a capacidade de armazenamento do disco com os seus arquivos e softwares e o usuário poderá escolher qual deseja iniciar ao ligar o computador.



Principais ferramentas:

A distribuição possui mais de 300 ferramentas nativas exclusivas para atividades de segurança e pentests. O Kali Linux inclui por padrão ferramentas como:

Metasploit: O Metasploit ajuda as equipes de segurança a verificar vulnerabilidades, gerenciar avaliações de segurança e melhorar a conscientização sobre segurança.

Nmap: O Nmap é útil para tarefas como inventário de rede, gerenciamento de agendamentos de atualização de serviços e monitoramento do tempo de atividade do host ou do serviço.

Wireshark: O Wireshark permite que você observe o que está acontecendo em sua rede em um nível "microscópico". É o analisador de protocolo de rede padrão em muitas empresas comerciais e sem fins lucrativos, agências governamentais e instituições educacionais.

Aircrack-ng: Aircrack-ng é um conjunto completo de ferramentas para avaliar a segurança da rede WiFi. Ele se concentra em diferente áreas de segurança WiFi:

- Monitoramento
- Ataque
- Teste
- Cracking

Fontes:

- https://diolinux.com.br/tecnologia/kali-linux.htm;
- https://www.aircrack-ng.org/;
- https://www.metasploit.com/;
- https://diolinux.com.br/tecnologia/kali-linux.htm;
- https://nmap.org/;
- https://www.cisoadvisor.com.br/kali-linux-ganha-nova-distribuicao-para-seguranca-defensiva/;

Obrigado pela atenção!!