Análise Pericial em Sistemas Operacionais Linux

Rodrigo Lange

LABORATÓRIOS - COM RESPOSTAS

Versão 2025

IPOG

Instruções para execução dos laboratórios

IPOG

LABORATÓRIO

Módulo 01
Introdução aos sistemas de arquivos Linux

IPOG

LABORATÓRIO

Módulo 02
Informações de data e horário

IPOG

LABORATÓRIO

Módulo 03
Permissões de arquivos e pastas

IPOG

LABORATÓRIO

Módulo 04
Duplicação forense em Linux

IPOG

LABORATÓRIO

Módulo 05
Coleta de informações voláteis

IPOG

LABORATÓRIO

Módulo 06
Análise dos processos em execução: dump da memória

IPOG

LABORATÓRIO

Módulo 07
Montagem de imagens

IPOG

LABORATÓRIO

Módulo 08
Geração de linha do tempo (timeline)

IPOG

LABORATÓRIO

Módulo 09
Data Carving: procurando arquivos específicos

IPOG

ANEXOS

IPOG

LABORATÓRIO

Módulo 10
Estudo de caso: ferramentas de análise em sistemas Linux

IPOG

LABORATÓRIO

Módulo 11
Arquivos de Log

IPOG

LABORATÓRIO

Módulo 12
Outras fontes de informação em sistemas Linux

IPOG

LABORATÓRIO

Módulo 13
Estudo de Vulnerabilidades

IPOG

IPOG

Instruções para execução dos laboratórios

Instruções para execução dos laboratórios

- Devem ser seguidas as instruções para **anexar** à máquina virtual do Kali o arquivo de imagem "**imagem_laboratorio.vdi**".
- Para baixar o arquivo de imagem "**imagem_laboratorio.vdi**", o link está disponível em https://drive.google.com/file/d/1W9mXGMF4ia3wZP212mEUAknVJoGOy9kQ/view?usp=sharing
- Todas as referências de partições, volumes, arquivos e pastas referem-se ao **volume do laboratório**.

Instruções para execução dos laboratórios

1) Abrir o aplicativo **Virtual Box**.
2) Selecionar a máquina virtual do Kali
3) Clicar em "Configurações"
4) Clicar em "Armazenamento"
5) Clicar em "Controladora Sata"
6) Clicar no botão "Adiciona disco rígido."
7) Clicar no botão "Acrescentar"
8) Selecionar o arquivo "**imagem_laboratorio.vdi**"
9) Clicar no botão "Abrir"

Instruções para execução dos laboratórios

10) Clicar no arquivo de imagem "**imagem_laboratorio.vdi**"

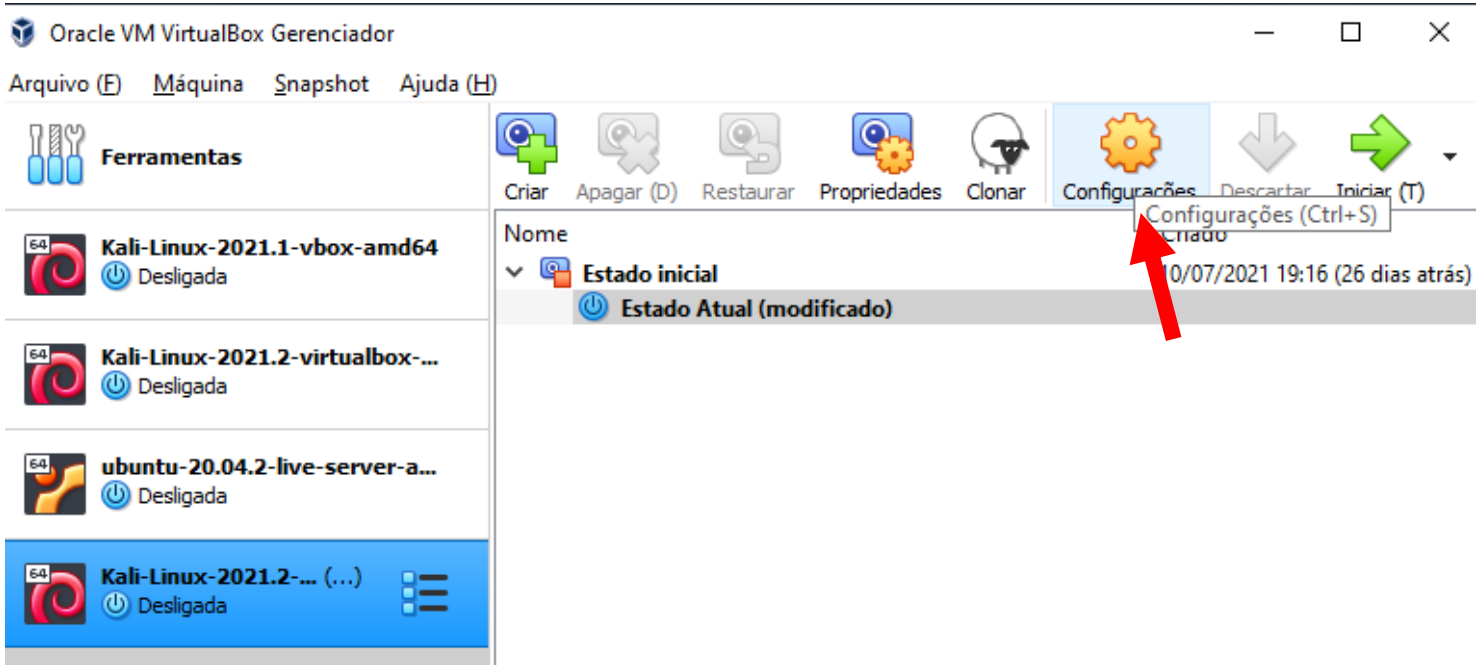
11) Clicar no botão "Escolher"

12) Clicar no botão "OK"

13) Clicar no botão "Iniciar (T)"

Instruções para execução dos laboratórios

1) Abrir o aplicativo **Virtual Box**.
2) Selecionar a máquina virtual do Kali
3) Clicar em "Configurações"

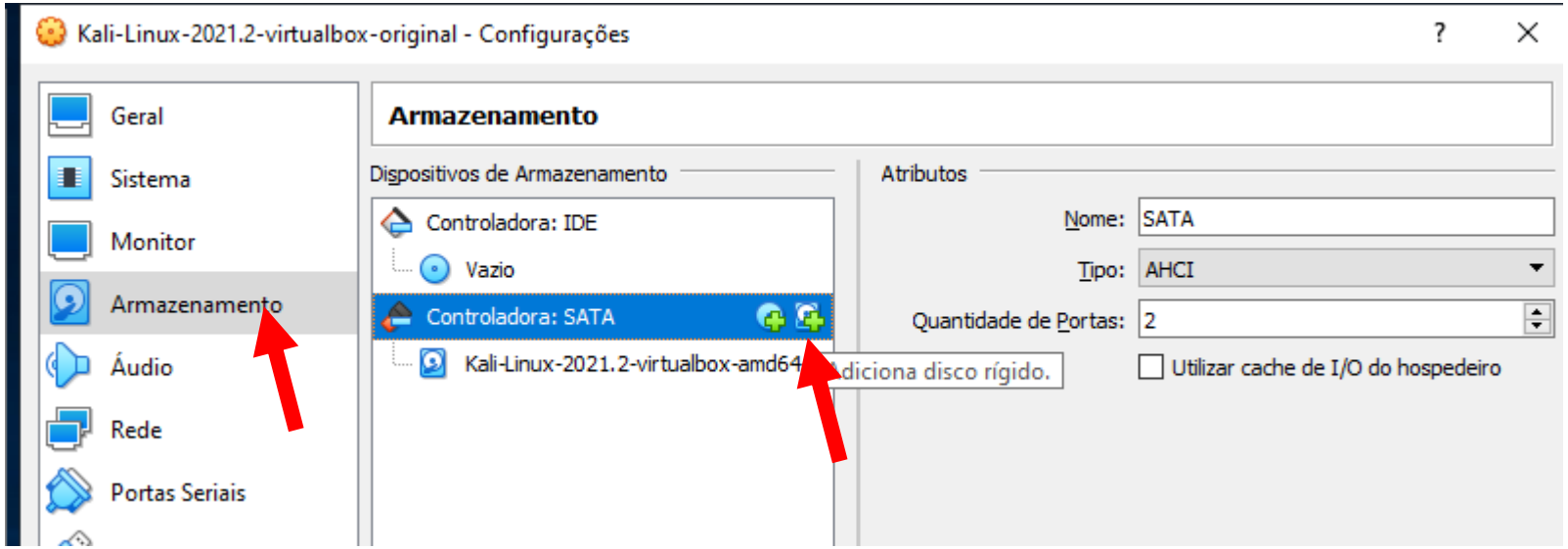


Instruções para execução dos laboratórios

4) Clicar em "Armazenamento"

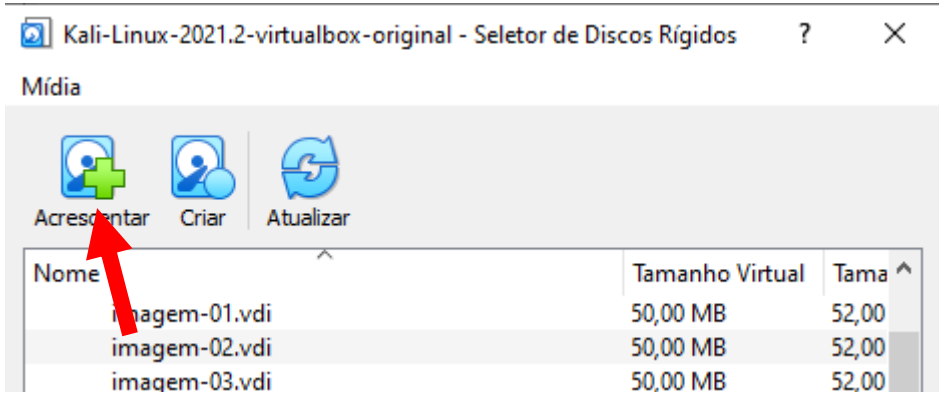
5) Clicar em "Controladora Sata"

6) Clicar no botão "Adiciona disco rígido."



Instruções para execução dos laboratórios

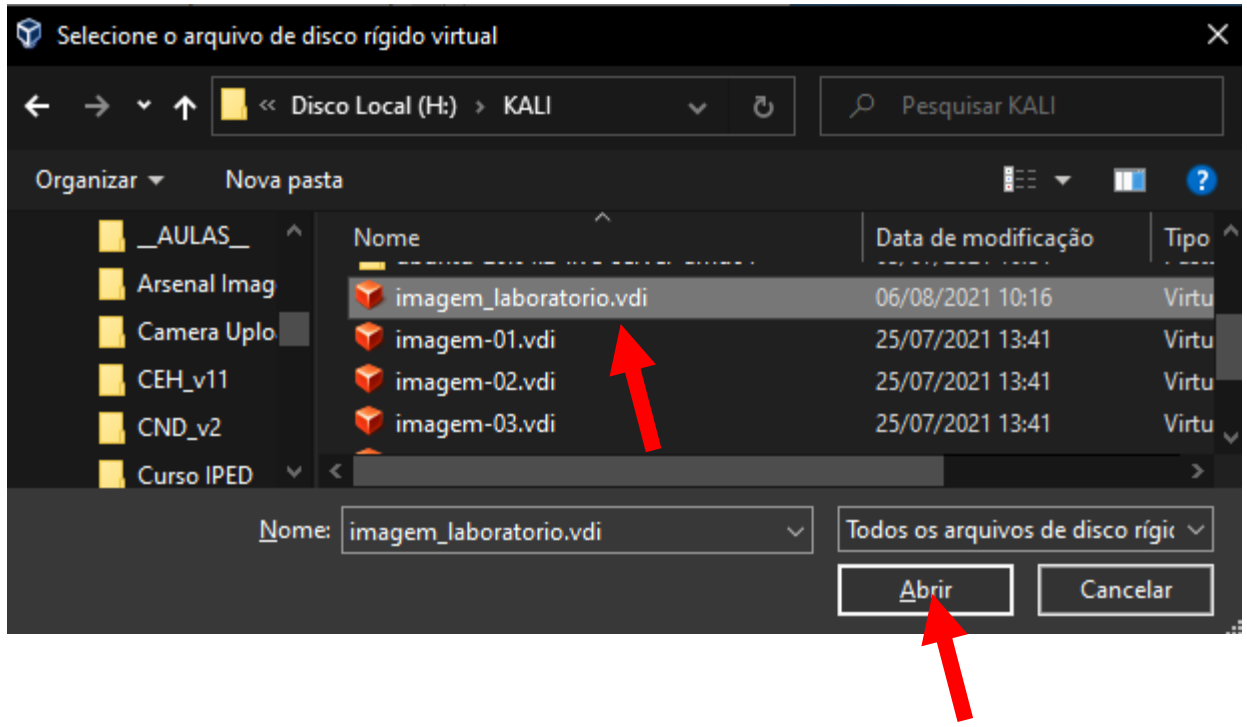
7) Clicar no botão "Acrescentar"



Instruções para execução dos laboratórios

8) Selecionar o arquivo "**imagem_laboratorio.vdi**"

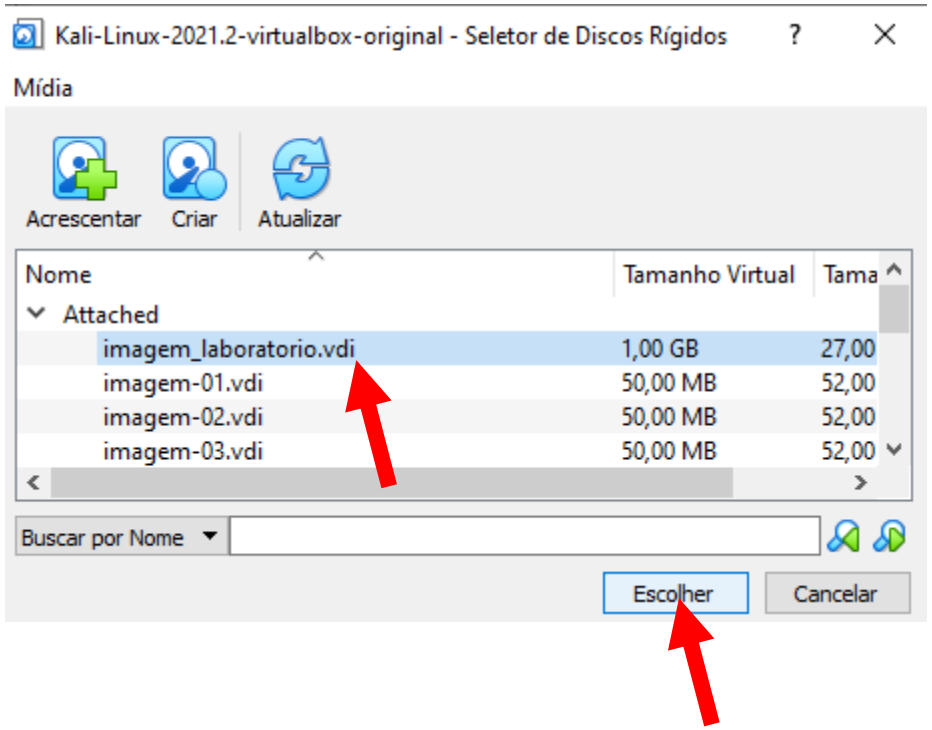
9) Clicar no botão "Abrir"



Instruções para execução dos laboratórios

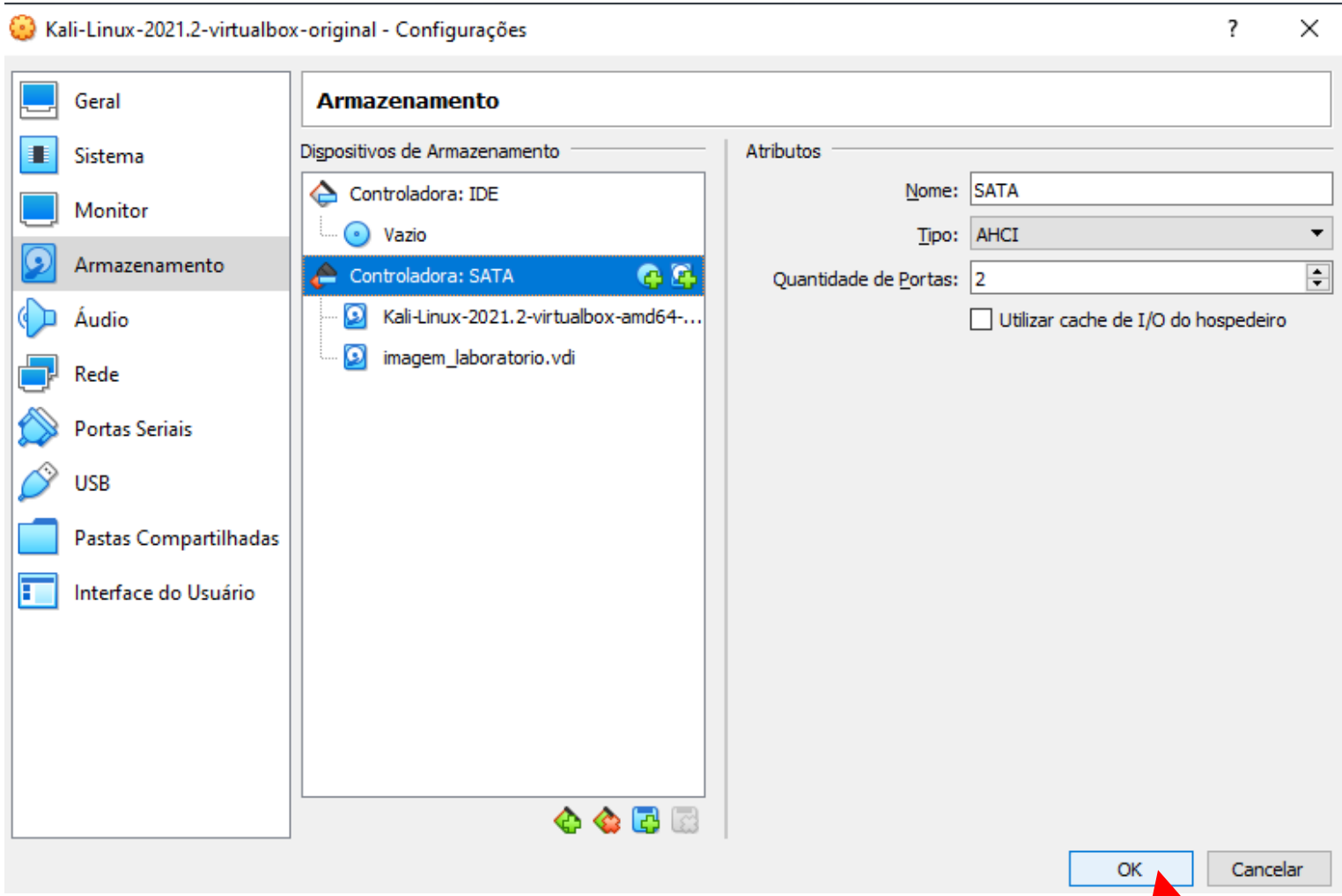
10) Clicar no arquivo de imagem "**imagem_laboratorio.vdi**"

11) Clicar no botão "Escolher"



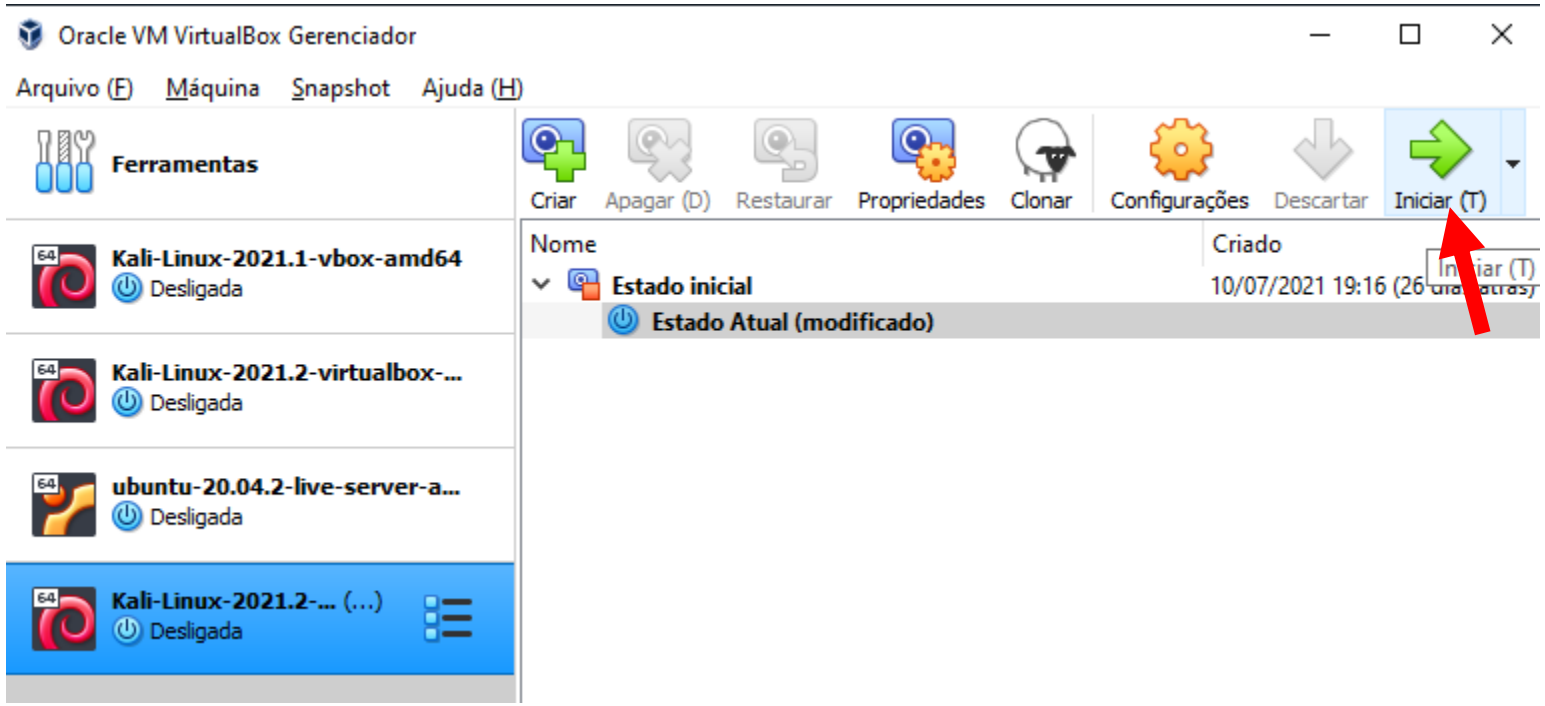
Instruções para execução dos laboratórios

12) Clicar no botão "OK"



Instruções para execução dos laboratórios

13) Clicar no botão "Iniciar (T)"



LABORATÓRIO

Módulo 01

Introdução aos sistemas de arquivos Linux

Laboratório - Módulo 1

Questão 1.1 - O disco de imagem do laboratório possui partições GPT ou MBR (msdos)?

(**X**) GPT

( ) MBR

Laboratório - Módulo 1

```
┌──(root💀kali)-[~/volatility]
└─# fdisk -l /dev/sdb
Disk /dev/sdb: 1 GiB, 1073741824 bytes, 2097152 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: 32FC098E-184D-471F-8EA7-2887F504F61A

Device       Start     End Sectors  Size Type
```

```
┌──(root💀kali)-[~/volatility]
└─# gdisk -l /dev/sdb
GPT fdisk (gdisk) version 1.0.6

Partition table scan:
  MBR: protective
  BSD: not present
  APM: not present
  GPT: present

Found valid GPT with protective MBR; using GPT.
Disk /dev/sdb: 2097152 sectors, 1024.0 MiB
Model: VBOX HARDDISK
Sector size (logical/physical): 512/512 bytes
Disk identifier (GUID): 32FC098E-184D-471F-8EA7-2887F504F61A
```

Laboratório - Módulo 1

Questão 1.2 - A controladora desse disco é:

(**X**) ATA/SATA

( ) SCSI

( ) FIREWIRE

( ) USB

Laboratório - Módulo 1

```
┌──(root💀kali)-[~/volatility]
└─# smartctl /dev/sdb -a
smartctl 7.2 2020-12-30 r5155 [x86_64-linux-5.10.0-kali9-amd64] (local build)
Copyright (C) 2002-20, Bruce Allen, Christian Franke, www.smartmontools.org

=== START OF INFORMATION SECTION ===
Device Model:     VBOX HARDDISK
Serial Number:    VB9b3c6193-764d0243
Firmware Version: 1.0
User Capacity:    1,073,741,824 bytes [1.07 GB]
Sector Size:      512 bytes logical/physical
Device is:        Not in smartctl database [for details use: -P showall]
ATA Version is:   ATA/ATAPI-6 published, ANSI INCITS 361-2002
Local Time is:    Sat Aug  7 22:00:28 2021 -03
SMART support is: Unavailable - device lacks SMART capability.
```

```
┌──(root💀kali)-[~/volatility]
└─# lsscsi
[1:0:0:0]    cd/dvd  VBOX     CD-ROM           1.0   /dev/sr0
[2:0:0:0]    disk    ATA      VBOX HARDDISK    1.0   /dev/sda
[3:0:0:0]    disk    ATA      VBOX HARDDISK    1.0   /dev/sdb
```

Laboratório - Módulo 1

Questão 1.3 - Identifique o sistema de arquivos das partições 1 a 6:

Partição 1: **ext2**

Partição 2: **ext3**

Partição 3: **ext4**

Partição 4: **vfat (FAT16)**

Partição 5: **exfat**

Partição 6: **ntfs**

Laboratório - Módulo 1

```
┌──(root💀kali)-[~/volatility]
└─# lsblk -f /dev/sdb
NAME   FSTYPE FSVER LABEL UUID                                 FSAVAIL FSUSE% MOUNTPOINT
sdb
├─sdb1 ext2   1.0         6311a8bb-73c2-44aa-8071-ae5d4ffa8e7c
├─sdb2 ext3   1.0         f222f88a-cb56-4bab-86ea-66b898587c9d
├─sdb3 ext4   1.0         5fec092b-29f5-4ffa-a569-784dad6df3a3
├─sdb4 vfat   FAT16       796B-5AED
├─sdb5 exfat  1.0         79C8-AF1E
└─sdb6 ntfs               7EB6E1FE764C3F70                      237.5M    73% /mnt/analise
```

Laboratório - Módulo 1

Questão 1.4 - Identifique o tamanho total das partições 1 a 6:

Partição 1: **30 MB**

Partição 2: **30 MB**

Partição 3: **30 MB**

Partição 4: **30 MB**

Partição 5: **30 MB**

Partição 6: **873 MB**

Laboratório - Módulo 1

Laboratório - Módulo 1

Questão 1.5 - Confira a integridade das partições 1 a 6. Alguma apresentou erro?

Partição 1: **Sem erros**

Partição 2: **Sem erros**

Partição 3: **Sem erros**

Partição 4: **Sem erros**

Partição 5: **Sem erros**

Partição 6: **Sem erros**

Laboratório - Módulo 1

```
┌──(root💀kali)-[~/volatility]
└─# fsck /dev/sdb1
fsck from util-linux 2.36.1
e2fsck 1.46.2 (28-Feb-2021)
/dev/sdb1: clean, 11/7680 files, 1346/30720 blocks

┌──(root💀kali)-[~/volatility]
└─# fsck /dev/sdb2
fsck from util-linux 2.36.1
e2fsck 1.46.2 (28-Feb-2021)
/dev/sdb2: clean, 11/7680 files, 2375/30720 blocks

┌──(root💀kali)-[~/volatility]
└─# fsck /dev/sdb3
fsck from util-linux 2.36.1
e2fsck 1.46.2 (28-Feb-2021)
/dev/sdb3: clean, 11/7680 files, 2730/30720 blocks

┌──(root💀kali)-[~/volatility]
└─# fsck /dev/sdb4
fsck from util-linux 2.36.1
fsck.fat 4.2 (2021-01-31)
/dev/sdb4: 0 files, 0/15317 clusters
```

```
┌──(root💀kali)-[~/volatility]
└─# fsck /dev/sdb5
fsck from util-linux 2.36.1
exfatfsck 1.3.0
Checking file system on /dev/sdb5.
File system version           1.0
Sector size                 512 bytes
Cluster size                  4 KB
Volume size                  30 MB
Used space                  112 KB
Available space              30 MB
Totally 0 directories and 0 files.
File system checking finished. No errors found.

┌──(root💀kali)-[~/volatility]
└─# ntfsfix /dev/sdb6
Mounting volume... OK
Processing of $MFT and $MFTMirr completed successfully.
Checking the alternate boot sector... OK
NTFS volume version is 3.1.
NTFS partition /dev/sdb6 was processed successfully.
```

LABORATÓRIO

Módulo 02

Informações de data e horário

Laboratório - Módulo 2

Questão 2.1 - Quais são os parâmetros do comando "date" utilizados para gerar o formato da seguinte saída:

25/07/2021-17:16:17

Parâmetros: **date +%d/%m/%Y-%H:%M:%S**

Laboratório - Módulo 2

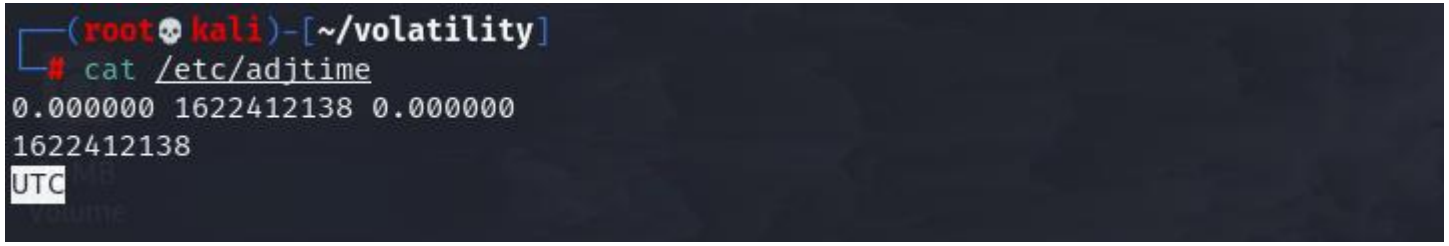
- **Questão 2.2** - O relógio de hardware do computador registra o horário no fuso local ou no fuso UTC? Qual arquivo foi consultado e ele está localizado em qual pasta (arquivo criado com a execução do comando hwclock --systohc)?

  ( ) LOCAL

  (**X**) UTC

  Arquivo consultado: **/etc/adjtime**

Laboratório - Módulo 2



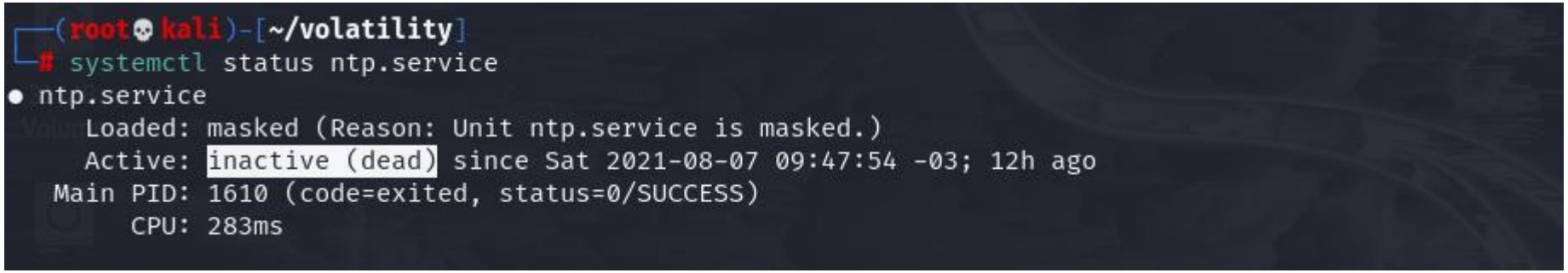
Laboratório - Módulo 2

- **Questão 2.3** - No Kali, o serviço de NTP está habilitado por padrão?

  ( ) SIM

  (**X**) NÃO

Laboratório - Módulo 2

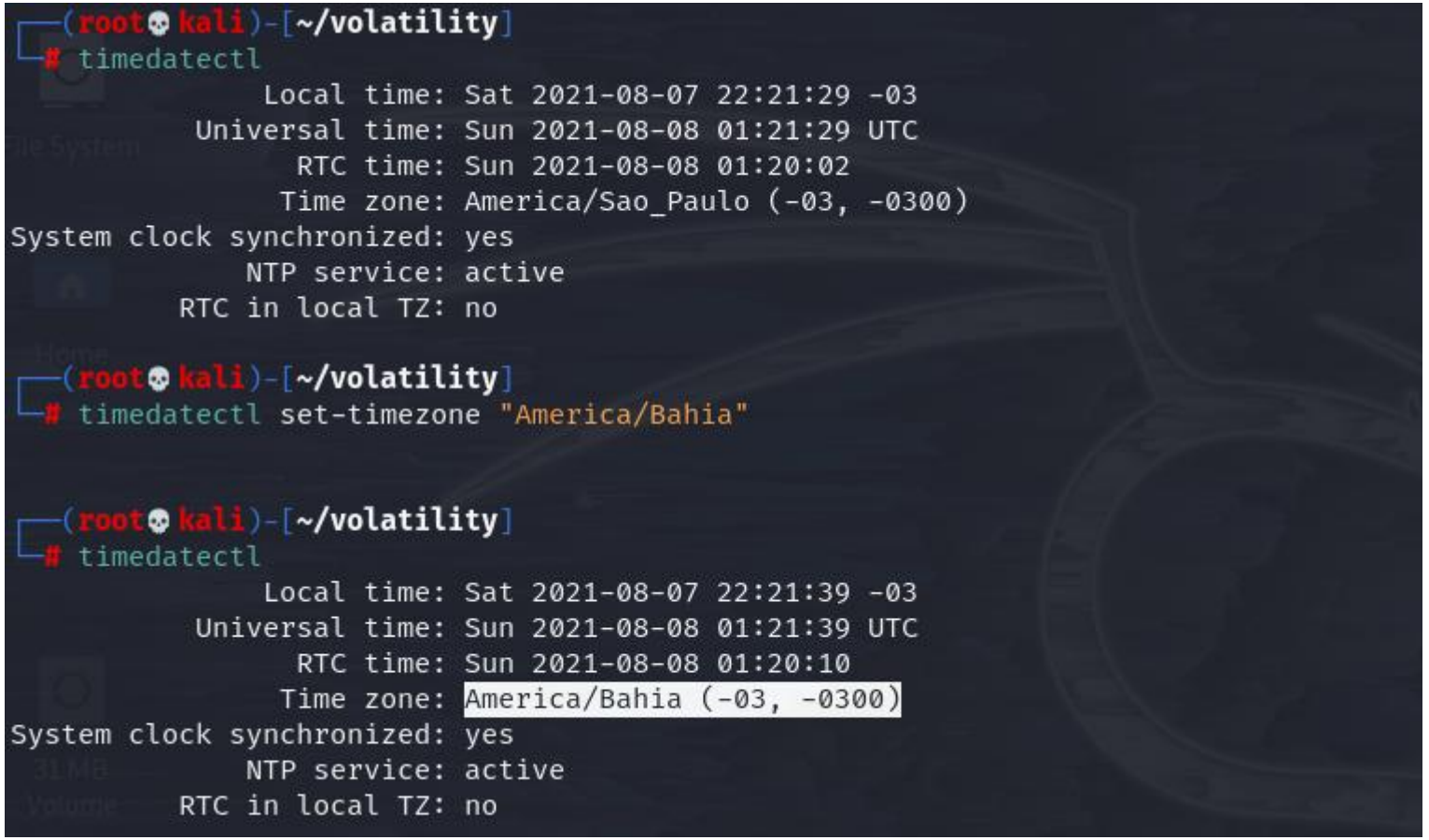


Laboratório - Módulo 2

- **Questão 2.4** - Qual comando e parâmetros devem ser utilizados para mudar o fuso horário para Bahia?

timedatectl set-timezone "America/Bahia"

Laboratório - Módulo 2



Laboratório - Módulo 2

- **Questão 2.5** - Quais os parâmetros devem ser utilizados com o comando "find" para encontrar todos arquivos modificados após o dia "05/08/2021"?

find . -type f -newermt "2021-08-05"

Laboratório - Módulo 2

LABORATÓRIO

Módulo 03

Permissões de arquivos e pastas

Laboratório - Módulo 3

Questão 3.1 - Em relação às permissões do arquivo "/etc/passwd", qual usuário consegue gravar informações nesse arquivo? Quais são as permissões desse usuário?

root - r (read) w (write)

Laboratório - Módulo 3

Laboratório - Módulo 3

Questão 3.2 - Ainda em relação às permissões do arquivo "/etc/passwd", o grupo do proprietário (owner) consegue gravar informações nesse arquivo?

( ) SIM

(**X**) NÃO

Laboratório - Módulo 3

Laboratório - Módulo 3

Questão 3.3 - Qual o tipo de arquivo de "/etc/localtime"?

( ) Pasta

(**X**) Link

( ) Conexão de rede

( ) Arquivo

Laboratório - Módulo 3

```
┌──(root💀kali)-[~/volatility]
└─# ls -la /etc/localtime
lrwxrwxrwx 1 root root 35 Aug  7 22:21 /etc/localtime → ../usr/share/zoneinfo/America/Bahia
```

Laboratório - Módulo 3

Questão 3.4 - Usando o comando "chmod" e a notação simbólica, qual dos comandos altera as permissões de um arquivo, identificado como [ARQUIVO], para permitir que o dono possa ler e gravar, mas não executar:

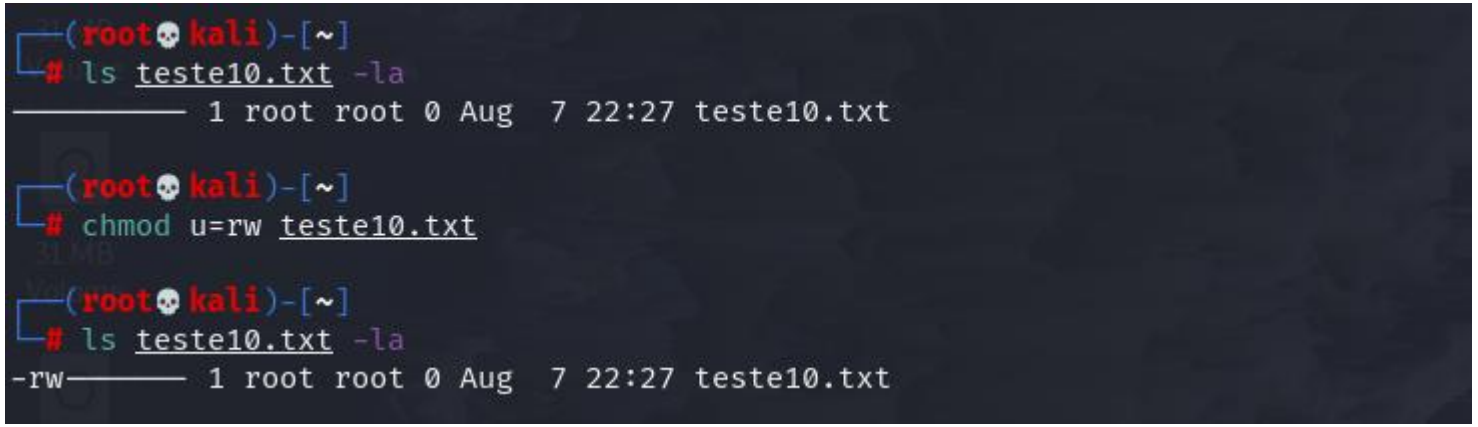
(**X**) chmod u=rw [ARQUIVO]

( ) chmod u=rwx [ARQUIVO]

( ) chmod u=x [ARQUIVO]

( ) chmod o=rw [ARQUIVO]

Laboratório - Módulo 3



Laboratório - Módulo 3

Questão 3.5 - Qual a sintaxe do comando "chattr" para habilitar o atributo somente leitura para um arquivo?

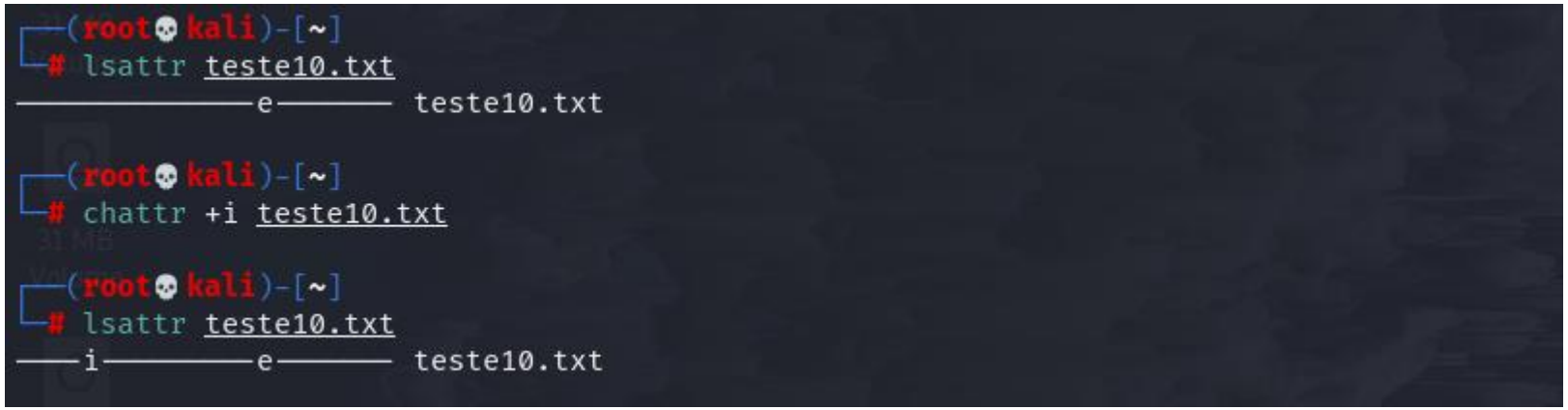
(**X**) chattr +i [ARQUIVO]

( ) chattr +a [ARQUIVO]

( ) chattr +d [ARQUIVO]

( ) chattr +s [ARQUIVO]

Laboratório - Módulo 3



LABORATÓRIO

Módulo 04

Duplicação forense em Linux

Laboratório - Módulo 4

Questão 4.1 - As funcionalidades HPA e DCO podem ser utilizadas para ocultar informações no disco rígido?

(**X**) VERDADEIRO

( ) FALSO

Laboratório - Módulo 4

Questão 4.2 - A sintaxe correta do comando "dd" para gerar um arquivo de imagem "destino.dd" de um disco rígido (sdb) com setor de tamanho de 512 bytes é:

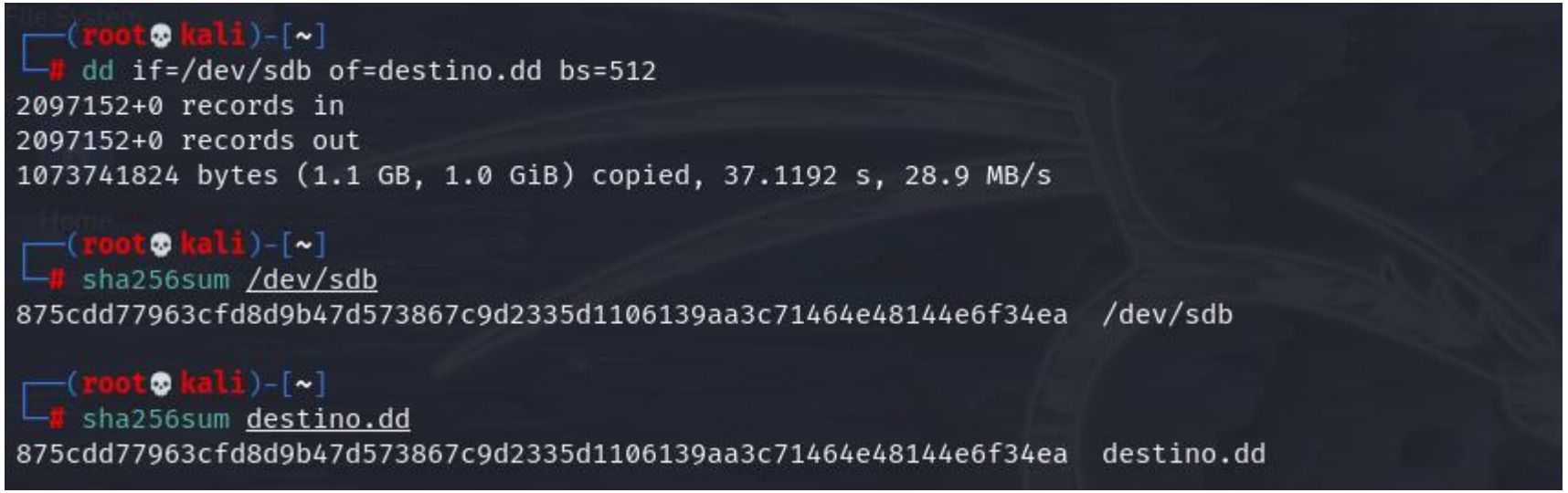
( ) dd of=/dev/sdb if=destino.dd bs=512

( ) dd if=/dev/sda of=destino.dd bs=512

( ) dd if=/dev/sdb1 of=destino.dd bs=512

(**X**) dd if=/dev/sdb of=destino.dd bs=512

Laboratório - Módulo 4



Laboratório - Módulo 4

Questão 4.3 - Quando a data e horário mantidos pelo sistema de arquivos do Sistema Operacional é alterado ou o nome do arquivo é modificado, o hash desse arquivo é alterado também?

( ) SIM

(**X**) NÃO

Laboratório - Módulo 4

Laboratório - Módulo 4

Questão 4.4 - Qual a sintaxe do comando "split" para segmentar o arquivo "imagem.dd" em tamanhos de 1 gigabyte e com extensão com 4 dígitos (.0000) e nome "imagem_segmentada."?

(**X**) split -d -a4 -b1G imagem.dd imagem_segmentada.

( ) split -d -a3 -b1G imagem.dd imagem_segmentada.

( ) split -d -a4 -b1000G imagem.dd imagem_segmentada.

( ) split -d -a3 -b1000M imagem.dd imagem_segmentada.

Laboratório - Módulo 4

```
┌──(root💀kali)-[~]
└─# split -d -a4 -b1G imagem.dd imagem_segmentada.
```

Laboratório - Módulo 4

Questão 4.5 - Qual a sintaxe do aplicativo "ddrescue" para gerar um arquivo de imagem "imagem.dd" do disco "sdb" e um arquivo de mapa mapa.txt.

( ) ddrescue imagem.dd /dev/sdb mapa.txt

( ) ddrescue /dev/sda imagem.dd mapa.txt

( ) ddrescue /etc/sdb imagem.dd mapa.txt

(**X**) ddrescue /dev/sdb imagem.dd mapa.txt

Laboratório - Módulo 4

```
┌──(root💀kali)-[~]
└─# apt install gddrescue
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following package was automatically installed and is no longer required:
  libopts25
Use 'apt autoremove' to remove it.
Suggested packages:
  ddrescueview
The following NEW packages will be installed:
  gddrescue
```

```
┌──(root💀kali)-[~]
└─# ddrescue /dev/sdb imagem.dd mapa.txt
GNU ddrescue 1.23
Press Ctrl-C to interrupt
Initial status (read from mapfile)
rescued: 31457 kB, tried: 0 B, bad-sector: 0 B, bad areas: 0

Current status
     ipos:    1073 MB, non-trimmed:        0 B,  current rate:  48496 kB/s
     opos:    1073 MB, non-scraped:        0 B,  average rate:  37224 kB/s
non-tried:        0 B,  bad-sector:        0 B,    error rate:       0 B/s
  rescued:    1073 MB,   bad areas:        0,        run time:         27s
pct rescued:  100.00%, read errors:        0,  remaining time:        n/a
                              time since last successful read:        n/a
Finished
```

Laboratório - Módulo 4

Questão 4.6 - Gere uma imagem com o dd da partição "sdb3". Qual o hash MD5?

MD5: **baf303d624365d446bfa99f2dbe8eb4f**

Observação: o hash é alterado após a execução do fsck.

Laboratório - Módulo 4

```
┌──(root💀kali)-[~]
└─# dd if=/dev/sdb3 of=imagem3.dd bs=512

61440+0 records in
61440+0 records out
31457280 bytes (31 MB, 30 MiB) copied, 0.412497 s, 76.3 MB/s

┌──(root💀kali)-[~]
└─# md5sum imagem3.dd

baf303d624365d446bfa99f2dbe8eb4f  imagem3.dd

┌──(root💀kali)-[~]
└─# fsck /dev/sdb3
fsck from util-linux 2.36.1
e2fsck 1.46.2 (28-Feb-2021)
/dev/sdb3: clean, 11/7680 files, 2730/30720 blocks

┌──(root💀kali)-[~]
└─# dd if=/dev/sdb3 of=imagem4.dd bs=512

61440+0 records in
61440+0 records out
31457280 bytes (31 MB, 30 MiB) copied, 0.383022 s, 82.1 MB/s

┌──(root💀kali)-[~]
└─# md5sum imagem4.dd

ef439dcafcec29d5e628fc423a933fa2  imagem4.dd
```

LABORATÓRIO

Módulo 05

Coleta de informações voláteis

Laboratório - Módulo 5

Questão 5.1 - Qual comando pode ser utilizado para mostrar como os pacotes de rede serão roteados (tabela de roteamento)?

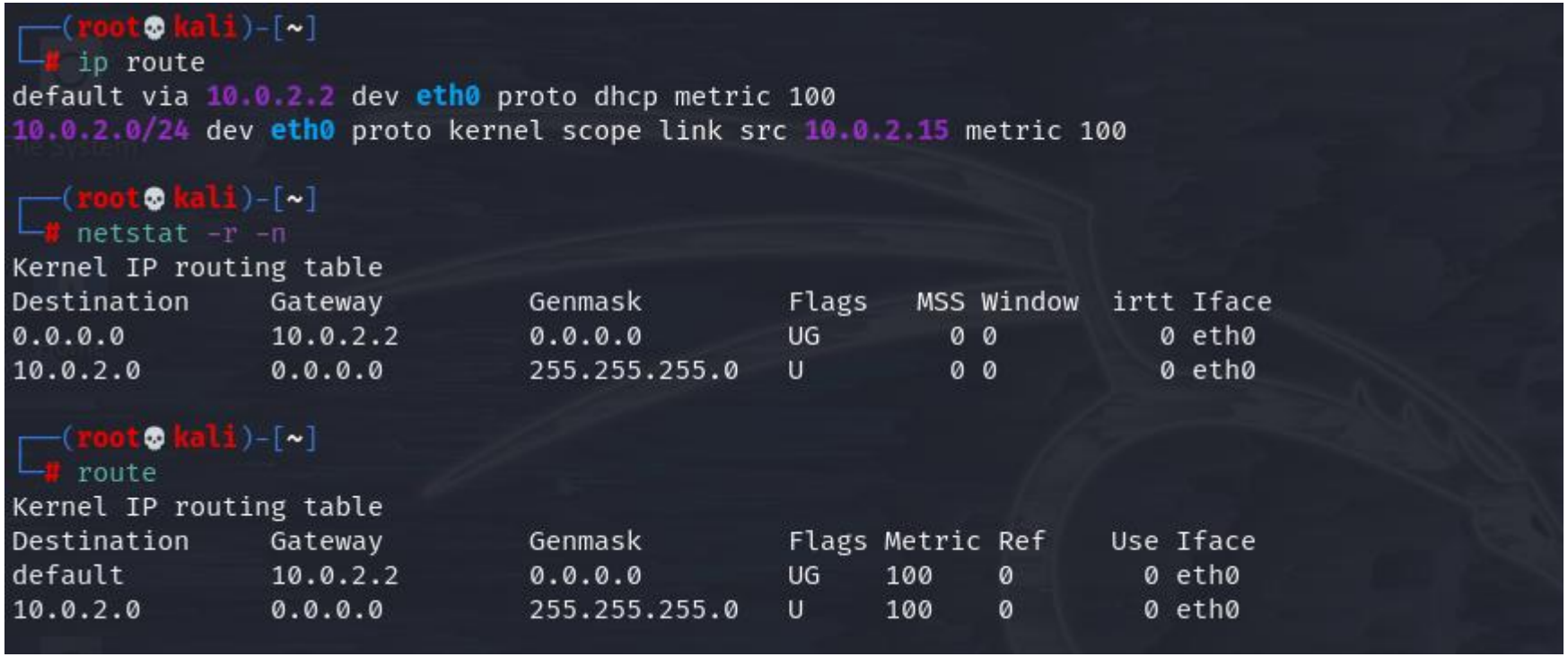
( ) ip route

( ) netstat -r -n

( ) route

(**X**) todos os comandos acima

Laboratório - Módulo 5



Laboratório - Módulo 5

Questão 5.2 - Qual o comando e parâmetros para identificar os registros de tradução entre um endereço IP e um endereço MAC?

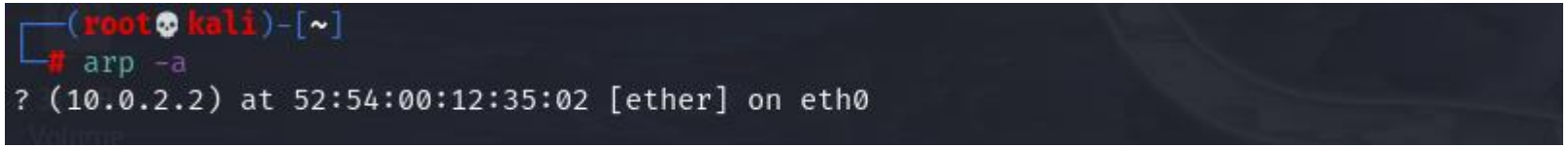
( ) arp -f

( ) arp -c

(**X**) arp -a

( ) ip cache arp

Laboratório - Módulo 5



Laboratório - Módulo 5

Questão 5.3 - Qual comando pode ser utilizado para identificar os usuários conectados?

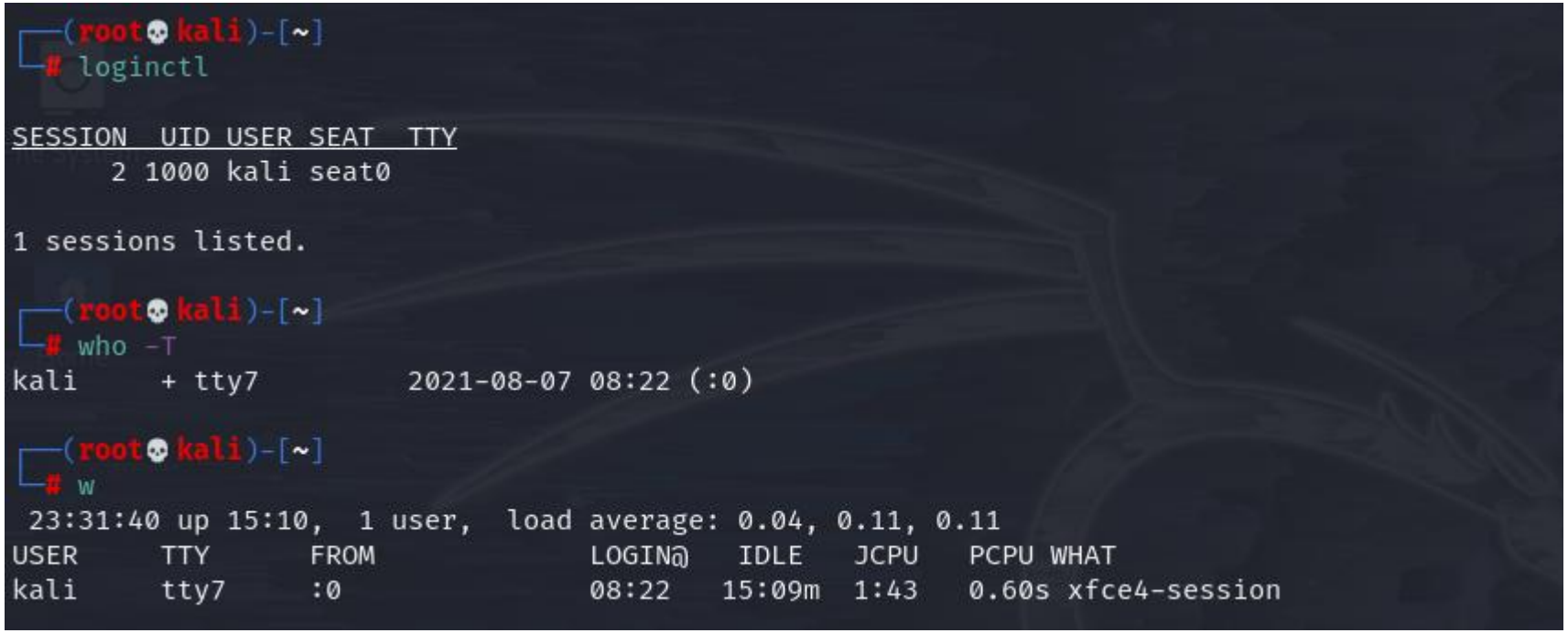
( ) loginctl

( ) who -T

( ) w

(**X**) todos os comandos acima

Laboratório - Módulo 5



Laboratório - Módulo 5

Questão 5.4 - Qual comando e parâmetros podem ser utilizados para identificar volumes cifrados (montados ou não)?

( ) cat /etc/crypttab

( ) lsblk -f

( ) mount -v

(X) todos os comandos acima

Laboratório - Módulo 5

```
┌──(root💀kali)-[~]
└─# cat /etc/crypttab
# <target name> <source device>         <key file>      <options>

┌──(root💀kali)-[~]
└─# lsblk -f
NAME   FSTYPE FSVER LABEL UUID                                 FSAVAIL FSUSE% MOUNTPOINT
sda
├─sda1 ext4   1.0         dff30eeb-7332-438d-964c-d5c7f4d357f7   59.5G    18% /
├─sda2
└─sda5 swap   1           730f5728-182d-4386-a03f-0576994c8d62                [SWAP]
sdb
├─sdb1 ext2   1.0         6311a8bb-73c2-44aa-8071-ae5d4ffa8e7c
├─sdb2 ext3   1.0         f222f88a-cb56-4bab-86ea-66b898587c9d
├─sdb3 ext4   1.0         5fec092b-29f5-4ffa-a569-784dad6df3a3
├─sdb4 vfat   FAT16       796B-5AED
├─sdb5 exfat  1.0         79C8-AF1E
└─sdb6 ntfs               7EB6E1FE764C3F70                    237.5M    73% /mnt/analise
sr0
```

Laboratório - Módulo 5

```
┌──(root💀kali)-[~]
└─# mount -v
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
udev on /dev type devtmpfs (rw,nosuid,relatime,size=979396k,nr_inodes=244849,mode=755)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
tmpfs on /run type tmpfs (rw,nosuid,nodev,noexec,relatime,size=203036k,mode=755)
/dev/sda1 on / type ext4 (rw,relatime,errors=remount-ro)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
tmpfs on /run/lock type tmpfs (rw,nosuid,nodev,noexec,relatime,size=5120k)
cgroup2 on /sys/fs/cgroup type cgroup2 (rw,nosuid,nodev,noexec,relatime,nsdelegate,memory_recursiveprot)
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)
none on /sys/fs/bpf type bpf (rw,nosuid,nodev,noexec,relatime,mode=700)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs (rw,relatime,fd=29,pgrp=1,timeout=0,minproto=5,maxproto=5,direct,pipe_ino=12388)
hugetlbfs on /dev/hugepages type hugetlbfs (rw,relatime,pagesize=2M)
mqueue on /dev/mqueue type mqueue (rw,nosuid,nodev,noexec,relatime)
debugfs on /sys/kernel/debug type debugfs (rw,nosuid,nodev,noexec,relatime)
tracefs on /sys/kernel/tracing type tracefs (rw,nosuid,nodev,noexec,relatime)
configfs on /sys/kernel/config type configfs (rw,nosuid,nodev,noexec,relatime)
fusectl on /sys/fs/fuse/connections type fusectl (rw,nosuid,nodev,noexec,relatime)
sunrpc on /run/rpc_pipefs type rpc_pipefs (rw,relatime)
binfmt_misc on /proc/sys/fs/binfmt_misc type binfmt_misc (rw,nosuid,nodev,noexec,relatime)
LINUX_FORENSE on /media/LF type vboxsf (rw,nodev,relatime)
tmpfs on /run/user/1000 type tmpfs (rw,nosuid,nodev,relatime,size=203032k,nr_inodes=50758,mode=700,uid=1000,gid=1000)
gvfsd-fuse on /run/user/1000/gvfs type fuse.gvfsd-fuse (rw,nosuid,nodev,relatime,user_id=1000,group_id=1000)
/dev/sdb6 on /mnt/analise type fuseblk (ro,relatime,user_id=0,group_id=0,allow_other,blksize=4096)
```

Laboratório - Módulo 5

Questão 5.5 - Qual a melhor forma de registrar as informações voláteis:

( ) confiar na memória do perito

( ) anotar em um papel

( ) filmar a tela

(**X**) gerar arquivos com os comandos executados e os resultados gerados

Laboratório - Módulo 5

Questão 5.6 - O arquivo "/var/log/lightdm/x-0.log" está sendo utilizado?

(**X**) SIM

( ) NÃO

Laboratório - Módulo 5

```
┌──(root㉿kali)-[~]
└─# lsof | grep '/var/log/lightdm/x-0.log'
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
      Output information may be incomplete.
lsof: WARNING: can't stat() fuse.portal file system /run/user/1000/doc
      Output information may be incomplete.
Xorg        678                        root    1w      REG                8,1        843    5112096 /var/log/lightdm/x-0.log
Xorg        678                        root    2w      REG                8,1        843    5112096 /var/log/lightdm/x-0.log
Xorg        678    696 InputThre       root    1w      REG                8,1        843    5112096 /var/log/lightdm/x-0.log
Xorg        678    696 InputThre       root    2w      REG                8,1        843    5112096 /var/log/lightdm/x-0.log
```

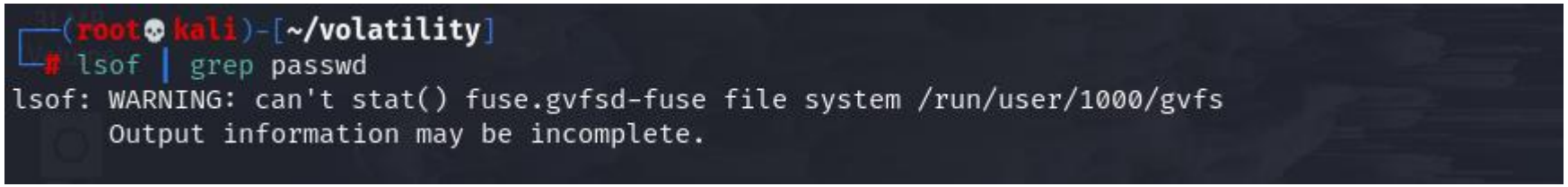
Laboratório - Módulo 5

Questão 5.7 - O arquivo "/etc/passwd" está sendo utilizado (está aberto)?

( ) SIM

(**X**) NÃO

Laboratório - Módulo 5



Laboratório - Módulo 5

Questão 5.8 - Qual o tipo do descritor do arquivo (*file descriptor*) de "/usr/bin/lsof"?

( ) cwd

(**X**) txt

( ) mem

( ) mmap

Laboratório - Módulo 5

```
┌──(root💀kali)-[~/volatility]
└─# lsof | grep /usr/bin/lsof
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
      Output information may be incomplete.
lsof       6064                          root  txt       REG               8,1     171488     533104 /usr/bin/lsof
lsof       6066                          root  txt       REG               8,1     171488     533104 /usr/bin/lsof
```

Laboratório - Módulo 5

Questão 5.9 - Quantas threads estão usando o arquivo " /var/log/lightdm/x-0.log"?

( ) 1

( ) 2

( ) 3

(**X**) 4

Laboratório - Módulo 5

```
┌──(root㉿kali)-[~]
└─# lsof | grep '/var/log/lightdm/x-0.log' | cat -n
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
      Output information may be incomplete.
lsof: WARNING: can't stat() fuse.portal file system /run/user/1000/doc
      Output information may be incomplete.
     1  Xorg        678                    root    1w      REG               8,1      883    5112096 /var/log/lightdm/x-0.log
     2  Xorg        678                    root    2w      REG               8,1      883    5112096 /var/log/lightdm/x-0.log
     3  Xorg        678    696 InputThre   root    1w      REG               8,1      883    5112096 /var/log/lightdm/x-0.log
     4  Xorg        678    696 InputThre   root    2w      REG               8,1      883    5112096 /var/log/lightdm/x-0.log
```

LABORATÓRIO

Módulo 06

Análise dos processos em execução: dump da memória

Laboratório - Módulo 6

Questão 6.1 - Não há riscos em acessar, alterar e copiar o conteúdo da memória RAM de um computador rodando Sistema Operacional Linux?

(**X**) FALSO

( ) VERDADEIRO

Laboratório - Módulo 6

Questão 6.2 - Quais arquivos dentro de "/proc/[PID]/" contêm informações sobre a linha de comando executada?

( ) "mem" e "kmem"

( ) "cmdline" e "command"

(**X**) "cmdline" e "comm"

( ) todos os arquivos acima

Laboratório - Módulo 6

Laboratório - Módulo 6

Questão 6.3 - É um processo pericial recomendável para cópia do conteúdo da memória RAM de um computador sendo examinado:

( ) baixar todos os aplicativos no computador

( ) compilar todos os aplicativos necessários

( ) fazer vários testes na própria máquina

(**X**) fazer uma cópia forense dos arquivos cifrados antes de tentar coletar a memória RAM

Laboratório - Módulo 6

Questão 6.4 - A ferramenta LIME exige a criação de um objeto de Kernel (.ko) que deve ser carregado pelo Kernel para geração do dump. Para isso é necessário compilar vários módulos. Para alterar o mínimo possível, pode-se gerar esse arquivo .ko em um computador idêntico ao examinado:

( ) FALSO

(**X**) VERDADEIRO

Laboratório - Módulo 6

Questão 6.5 - O plugin do Volatility que apresenta informações sobre os volumes montados no Linux é:

( ) mount_linux

( ) list_mount

(X) linux_mount

( ) linux_mount_list

Laboratório - Módulo 6

Questão 6.6 - **INSTRUÇÕES:**

1) Criar a pasta "/mnt/analise" (mkdir /mnt/analise)
2) Montar o dispositivo /dev/sdb6 somente leitura (mount -r -o ro,loop /dev/sdb6 /mnt/analise)

Laboratório - Módulo 6

Questão 6.6 - Execute o Volatility sobre o arquivo “/mnt/analise/linux-sample.bin” usando o profile “Linuxprofilex64” e cite três pastas entre as que estavam montadas com base no arquivo de imagem de memória :

Pasta 1: **/dev**

Pasta 2: **/run**

Pasta 3: **/run/shm**

Laboratório - Módulo 6

```
┌──(root㉿kali)-[/mnt/analise]
└─# vol.py -f /mnt/analise/linux-sample.bin --profile=Linuxprofilex64 linux_mount
Volatility Foundation Volatility Framework 2.6.1
/dev/disk/by-uuid/8f2bb477-848b-4bcb-9173-fd2f982db24d /                                 ext4         rw,relatime

udev                    /dev                            devtmpfs     rw,relatime
tmpfs                   /run                            tmpfs        rw,relatime,nosuid,noexec
tmpfs                   /run/shm                        tmpfs        rw,relatime,nosuid,nodev,noexec
proc                    /proc                           proc         rw,relatime,nosuid,nodev,noexec
rpc_pipefs              /var/lib/nfs/rpc_pipefs         rpc_pipefs   rw,relatime
sysfs                   /sys                            sysfs        rw,relatime,nosuid,nodev,noexec
binfmt_misc             /proc/sys/fs/binfmt_misc        binfmt_misc  rw,relatime,nosuid,nodev,noexec
devpts                  /dev/pts                        devpts       rw,relatime,nosuid,noexec
tmpfs                   /run/lock                       tmpfs        rw,relatime,nosuid,nodev,noexec
```

LABORATÓRIO

Módulo 07

Montagem de imagens

Laboratório - Módulo 7

INSTRUÇÕES

1) criar uma pasta como local de destino da montagem
2) identificar o início da partição (se for imagem de disco)
3) identificar o sistema de arquivos
4) montar a partição
5) realizar a análise
6) desmontar a partição

Laboratório - Módulo 7

INSTRUÇÕES

1) Criar a pasta "/mnt/teste1" (mkdir /mnt/teste1)
2) Caso não exista, crie a pasta "/mnt/analise" (mkdir /mnt/analise)
3) Caso não esteja montado, monte o dispositivo sdb6 em "/mnt/analise" com permissão apenas de leitura (mount -r -o ro,loop /dev/sdb6 /mnt/analise)

Laboratório - Módulo 7

Questão 7.1 - Identifique quantas partições existem no arquivo de imagem "/mnt/analise/imagem.dd".

( ) 1

(**X**) 2

( ) 3

( ) 4

Laboratório - Módulo 7

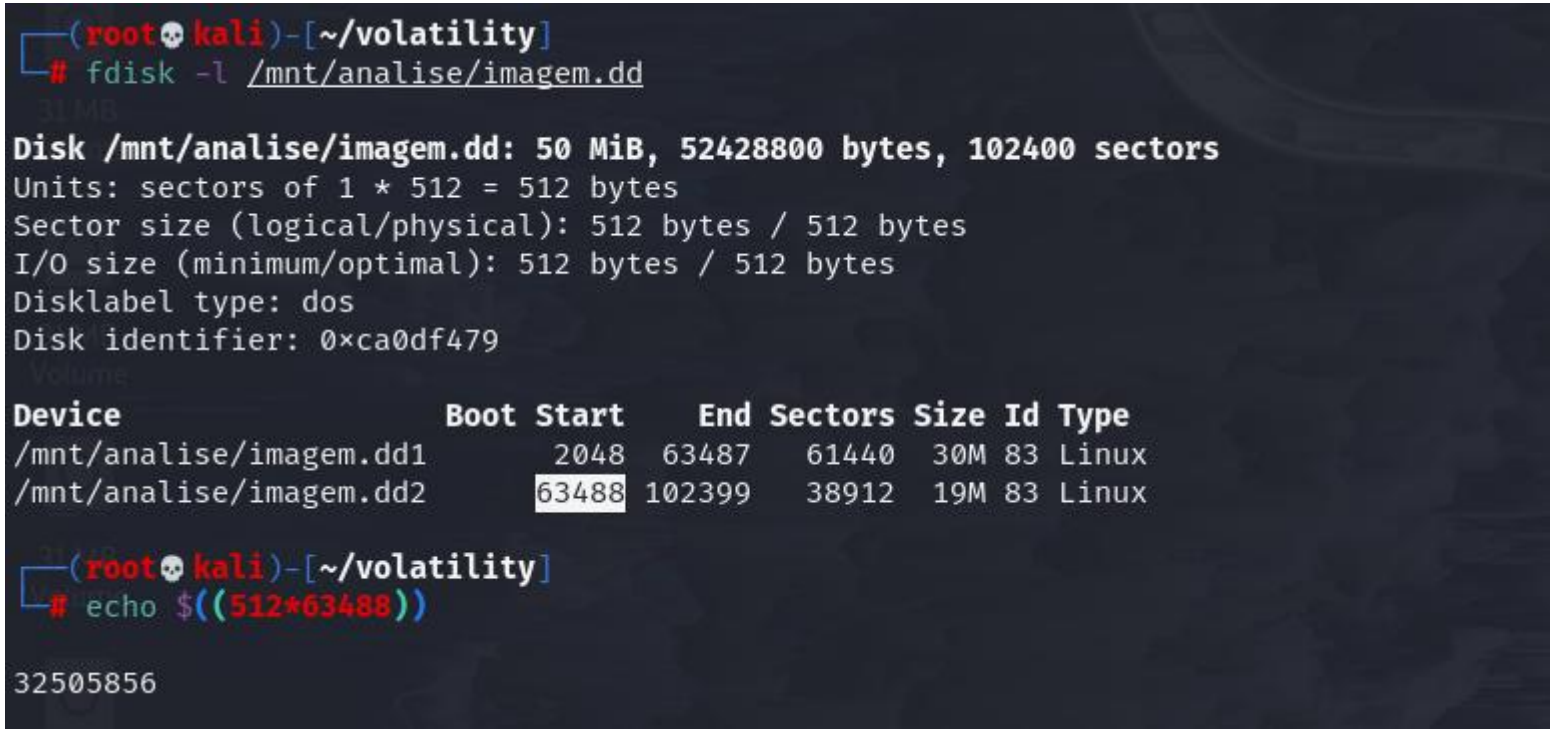
```
┌──(root💀kali)-[~/volatility]
└─# fdisk -l /mnt/analise/imagem.dd

Disk /mnt/analise/imagem.dd: 50 MiB, 52428800 bytes, 102400 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xca0df479

Device                    Boot Start    End Sectors Size Id Type
/mnt/analise/imagem.dd1         2048  63487   61440  30M 83 Linux
/mnt/analise/imagem.dd2        63488 102399   38912  19M 83 Linux
```

Laboratório - Módulo 7

Questão 7.2 - Qual o offset **em bytes** de início da segunda partição do arquivo de imagem "/mnt/analise/imagem.dd"?

Offset (em bytes): **512 * 63488 = 32505856**

Laboratório - Módulo 7



Laboratório - Módulo 7

Questão 7.3 - Qual o sistema de arquivos da segunda partição do arquivo de imagem "/mnt/analise/imagem.dd"?

Sistema de arquivos: **ext2**

Laboratório - Módulo 7

```
┌──(root💀kali)-[/mnt/analise]
└─# disktype imagem.dd

--- imagem.dd
Regular file, size 50 MiB (52428800 bytes)
DOS/MBR partition map
Partition 1: 30 MiB (31457280 bytes, 61440 sectors from 2048)
  Type 0×83 (Linux)
  Ext2 file system
    UUID 79CC7F87-2A58-438B-BC32-8E0C30783D06 (DCE, v4)
    Volume size 30 MiB (31457280 bytes, 30720 blocks of 1 KiB)
Partition 2: 19 MiB (19922944 bytes, 38912 sectors from 63488)
  Type 0×83 (Linux)
  Ext2 file system
    UUID A901A22E-4487-450C-B06B-5EE6C6BF9F66 (DCE, v4)
    Last mounted at "/mnt/teste1"
    Volume size 19 MiB (19922944 bytes, 19456 blocks of 1 KiB)
```

Laboratório - Módulo 7

Questão 7.4 - Qual a sintaxe do comando "mount" para montar a segunda partição do arquivo de imagem "/mnt/analise/imagem.dd" em "/mnt/teste1" no modo somente leitura?

mount -r -o ro,loop,offset=32505856 /mnt/analise/imagem.dd /mnt/teste1

Laboratório - Módulo 7

```
┌──(root💀kali)-[/mnt/analise]
└─# mount -r -o ro,loop,offset=32505856 /mnt/analise/imagem.dd /mnt/teste1
```

Laboratório - Módulo 7

Questão 7.5 - Qual o conteúdo do arquivo "/mnt/teste1/codigo.txt"?

Conteúdo do arquivo: **123456**

Laboratório - Módulo 7

LABORATÓRIO

Módulo 08

Geração de linha do tempo (timeline)

IPOG

Laboratório - Módulo 8

Questão 8.1 - Gere com o "fls" um arquivo no formato "body file" do dispositivo sdb6. Quantas linhas foram geradas?

116

Laboratório - Módulo 8

```
┌──(root💀kali)-[~]
└─# fls -r -m / /dev/sdb6 > ~/lista_fls.txt


┌──(root💀kali)-[~]
└─# cat ~/lista_fls.txt -n

     1  0|/$AttrDef ($FILE_NAME)|4-48-2|r/rr-xr-xr-x|48|0|82|1627232175|1627232175|1627232175|1627232175
     2  0|/$AttrDef|4-128-1|r/rr-xr-xr-x|48|0|2560|1627232175|1627232175|1627232175|1627232175
     3  0|/$BadClus ($FILE_NAME)|8-48-3|r/rr-xr-xr-x|0|0|82|1627232175|1627232175|1627232175|1627232175
     4  0|/$BadClus|8-128-2|r/rr-xr-xr-x|0|0|0|1627232175|1627232175|1627232175|1627232175
     5  0|/$BadClus:$Bad|8-128-1|r/rr-xr-xr-x|0|0|915386368|1627232175|1627232175|1627232175|1627232175
     6  0|/$Bitmap ($FILE_NAME)|6-48-2|r/rr-xr-xr-x|0|0|80|1627232175|1627232175|1627232175|1627232175
     7  0|/$Bitmap|6-128-1|r/rr-xr-xr-x|0|0|27936|1627232175|1627232175|1627232175|1627232175
     8  0|/$Boot ($FILE_NAME)|7-48-2|r/rr-xr-xr-x|48|0|76|1627232175|1627232175|1627232175|1627232175
```

```
   109  0|/$OrphanFiles/OrphanFile-16 (deleted)|16|-/rr-xr-xr-x|4294967295|0|0|1627232175|1627232175|1627232175|1627232175
   110  0|/$OrphanFiles/OrphanFile-17 (deleted)|17|-/rr-xr-xr-x|4294967295|0|0|1627232175|1627232175|1627232175|1627232175
   111  0|/$OrphanFiles/OrphanFile-18 (deleted)|18|-/rr-xr-xr-x|4294967295|0|0|1627232175|1627232175|1627232175|1627232175
   112  0|/$OrphanFiles/OrphanFile-19 (deleted)|19|-/rr-xr-xr-x|4294967295|0|0|1627232175|1627232175|1627232175|1627232175
   113  0|/$OrphanFiles/OrphanFile-20 (deleted)|20|-/rr-xr-xr-x|4294967295|0|0|1627232175|1627232175|1627232175|1627232175
   114  0|/$OrphanFiles/OrphanFile-21 (deleted)|21|-/rr-xr-xr-x|4294967295|0|0|1627232175|1627232175|1627232175|1627232175
   115  0|/$OrphanFiles/OrphanFile-22 (deleted)|22|-/rr-xr-xr-x|4294967295|0|0|1627232175|1627232175|1627232175|1627232175
   116  0|/$OrphanFiles/OrphanFile-23 (deleted)|23|-/rr-xr-xr-x|4294967295|0|0|1627232175|1627232175|1627232175|1627232175
```

Laboratório - Módulo 8

Questão 8.2 - Gere com o "ils" um arquivo no formato "body file" da segunda partição do arquivo de imagem "/mnt/analise/imagem2.dd". Quantas linhas foram geradas?

9

Laboratório - Módulo 8

```
┌──(root💀kali)-[~]
└─# fdisk -l /mnt/analise/imagem2.dd

Disk /mnt/analise/imagem2.dd: 50 MiB, 52428800 bytes, 102400 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: 9D9ED382-2EC6-45A2-9630-72C8A889D0EE

Device                     Start    End Sectors Size Type
/mnt/analise/imagem2.dd1    2048  63487   61440  30M Linux filesystem
/mnt/analise/imagem2.dd2   63488 102366   38879  19M Linux filesystem

┌──(root💀kali)-[~]
└─# ils /mnt/analise/imagem2.dd -o 63488 -r -m > ~/lista_ils.txt


┌──(root💀kali)-[~]
└─# cat ~/lista_ils.txt -n

     1  md5|file|st_ino|st_ls|st_uid|st_gid|st_size|st_atime|st_mtime|st_ctime|st_crtime
     2  0|<imagem2.dd-dead-16>|16|-/rr-xr-xr-x|4294967295|0|0|1623978752|1623978752|1623978752|1623978752
     3  0|<imagem2.dd-dead-17>|17|-/rr-xr-xr-x|4294967295|0|0|1623978752|1623978752|1623978752|1623978752
     4  0|<imagem2.dd-dead-18>|18|-/rr-xr-xr-x|4294967295|0|0|1623978752|1623978752|1623978752|1623978752
     5  0|<imagem2.dd-dead-19>|19|-/rr-xr-xr-x|4294967295|0|0|1623978752|1623978752|1623978752|1623978752
     6  0|<imagem2.dd-dead-20>|20|-/rr-xr-xr-x|4294967295|0|0|1623978752|1623978752|1623978752|1623978752
     7  0|<imagem2.dd-dead-21>|21|-/rr-xr-xr-x|4294967295|0|0|1623978752|1623978752|1623978752|1623978752
     8  0|<imagem2.dd-dead-22>|22|-/rr-xr-xr-x|4294967295|0|0|1623978752|1623978752|1623978752|1623978752
     9  0|<imagem2.dd-dead-23>|23|-/rr-xr-xr-x|4294967295|0|0|1623978752|1623978752|1623978752|1623978752
```

Laboratório - Módulo 8

Questão 8.3 - Execute o script "psteal.py" sobre o dispositivo sdb6 e gere o arquivo de linha do tempo "timeline.csv" (usando DOCKER). Quantas linhas foram geradas (incluindo cabeçalho)?

692

Laboratório - Módulo 8

```
┌──(root㉿kali)-[~]
└─# docker run --volume /mnt/:/mnt --device=/dev/sdb6 log2timeline/plaso psteal -w /mnt/linha_tempo.csv --source /dev/sdb6 -o dynamic
2024-07-01 17:08:45,825 [INFO] (MainProcess) PID:7 <artifact_definitions> Determined artifact definitions path: /usr/share/artifacts
Checking availability and versions of dependencies.
[OPTIONAL]      unable to determine version information for: flor
[OK]


Source path             : /dev/sdb6
Source type             : storage media device
Processing time         : 00:00:00

Processing started.
plaso - psteal version 20240308

Source path             : /dev/sdb6
Source type             : storage media device
Processing time         : 00:00:02

Identifier      PID     Status          Memory          Sources         Event Data      File
Main            7       collecting      138.2 MiB       1 (1)           0 (0)
```

Laboratório - Módulo 8

```
plaso - psteal version 20240308

Storage file            : 20240701T170847-sdb6.plaso
Processing time         : 00:00:01

Events:         Filtered        In time slice   Duplicates      MACB grouped    Total
                0               0               0               689             691

Identifier              PID     Status          Memory          Events          Tags            Reports
Main                    7       completed       139.8 MiB       691 (0)         0 (0)           0 (0)

Processing completed.
Storage file is: 20240701T170847-sdb6.plaso
```

Laboratório - Módulo 8

```
┌──(root㉿kali)-[~]
└─# wc -l /mnt/linha_tempo.csv
692 /mnt/linha_tempo.csv

┌──(root㉿kali)-[~]
└─# cat -n /mnt/linha_tempo.csv
     1  datetime,timestamp_desc,source,source_long,message,parser,display_name,tag
     2  1601-01-01T00:00:00.000000+00:00,Content Modification Time,FILE,File stat,NTFS:\$MFT Type: file,filestat,NTFS:\$MFT,-
     3  1601-01-01T00:00:00.000000+00:00,Creation Time,FILE,File stat,NTFS:\$MFT Type: file,filestat,NTFS:\$MFT,-
     4  1601-01-01T00:00:00.000000+00:00,Last Access Time,FILE,File stat,NTFS:\$MFT Type: file,filestat,NTFS:\$MFT,-
     5  1601-01-01T00:00:00.000000+00:00,Metadata Modification Time,FILE,File stat,NTFS:\$MFT Type: file,filestat,NTFS:\$MFT,-
     6  0000-00-00T00:00:00.000000+00:00,Not a time,FILE,NTFS file stat,NTFS:\$MFT File reference: 0-1 Attribute name: $STANDARD_INFORMATION Path
 hints: \$MFT,mft,NTFS:\$MFT,-
     7  0000-00-00T00:00:00.000000+00:00,Not a time,FILE,NTFS file stat,NTFS:\$MFTMirr File reference: 0-1 Attribute name: $STANDARD_INFORMATION
Path hints: \$MFT,mft,NTFS:\$MFTMirr,-
     8  2021-04-16T10:36:16.000000+00:00,Creation Time,PE,PE/COFF file,PE Type: Executable (EXE) Import hash: 6cde2f49ecf3cc2f14739babaa8fd75f,pe
,NTFS:\Aplicativos\WebBrowserPassView.exe,-
     9  2021-07-25T16:56:15.000000+00:00,Content Modification Time,FILE,File stat,NTFS:\$AttrDef Type: file,filestat,NTFS:\$AttrDef,-
    10  2021-07-25T16:56:15.000000+00:00,Creation Time,FILE,File stat,NTFS:\$AttrDef Type: file,filestat,NTFS:\$AttrDef,-
```

```
_INFORMATION Path hints: \Imagens\jpg,mft,NTFS:\$MFT,-
   689  2021-08-06T20:07:18.470429+00:00,Content Modification Time,FILE,File stat,NTFS:\Imagens\jpg Type: directory,filestat,NTFS:\Imagens\jpg,-
   690  2021-08-06T20:07:18.470429+00:00,Metadata Modification Time,FILE,File stat,NTFS:\Imagens\jpg Type: directory,filestat,NTFS:\Imagens\jpg,-
   691  2021-08-06T20:07:19.421366+00:00,Last Access Time,FILE,NTFS file stat,NTFS:\$MFT File reference: 83-1 Attribute name: $STANDARD_INFORMATI
ON Path hints: \Imagens\jpg,mft,NTFS:\$MFT,-
   692  2021-08-06T20:07:19.421366+00:00,Last Access Time,FILE,File stat,NTFS:\Imagens\jpg Type: directory,filestat,NTFS:\Imagens\jpg,-
```

LABORATÓRIO

Módulo 09

Data Carving: procurando arquivos específicos

Laboratório - Módulo 9

INSTRUÇÕES-

1) Crie as pastas "/mnt/teste3", "/mnt/teste4", "/mnt/teste5", "/mnt/teste6" e "/mnt/teste7" (mkdir /mnt/teste3 /mnt/teste4 /mnt/teste5 /mnt/teste6 /mnt/teste7)

Laboratório - Módulo 9

Questão 9.1 - Instale e execute o Foremost sobre o volume sdb6, salvando os arquivos recuperados em "/mnt/teste3". Quantos arquivos de imagem do tipo ".jpg" foram recuperados?

14

Laboratório - Módulo 9

```
┌──(root💀kali)-[~]
└─# apt install foremost
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following package was automatically installed and is no longer required:
  libopts25
Use 'apt autoremove' to remove it.
The following NEW packages will be installed:
  foremost
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 42.7 kB of archives.
```

```
┌──(root💀kali)-[~]
└─# foremost -i /dev/sdb6 -o /mnt/teste3

Processing: /dev/sdb6
|*foundat=module.dwarfUT
foundat=boot/System.map-3.2.0-4-amd64UT
*WMV err num_header_objs=-1801883236 headerSize=4821270156401102795
WMV err num_header_objs=-1073683314 headerSize=12834305435917262 41
WMV err num_header_objs=-1442784858 headerSize=12833571808698793 50
*******|

┌──(root💀kali)-[~]
└─# ls /mnt/teste3
audit.txt  exe  gif  jpg  pdf  png  wav  zip

┌──(root💀kali)-[~]
└─# ls /mnt/teste3/jpg
00223488.jpg  01494400.jpg  01555355.jpg  01586304.jpg  01717320.jpg  01750144.jpg  01756288.jpg
01493824.jpg  01495208.jpg  01555381.jpg  01685616.jpg  01718128.jpg  01755712.jpg  01782848.jpg
```

IPOG

Laboratório - Módulo 9

Questão 9.2 - Edite o arquivo "/etc/scalpel/scalpel.conf" e retire o símbolo de comentário ("#") dos arquivos do tipo ".jpg". Em seguida, execute o "scalpel" sobre o volume sdb6 e salve em "/mnt/teste4". Quantos arquivos de imagem do tipo ".jpg" foram recuperados?

14

Laboratório - Módulo 9

```
┌──(root💀kali)-[~]
└─# nano /etc/scalpel/scalpel.conf
```

```
# GIF and JPG files (very common)
#       gif     y       5000000         \x47\x49\x46\x38\x37\x61        \x00\x3b
#       gif     y       5000000         \x47\x49\x46\x38\x39\x61        \x00\x3b
        jpg     y       5242880         \xff\xd8\xff???Exif             \xff\xd9        REVERSE
        jpg     y       5242880         \xff\xd8\xff???JFIF             \xff\xd9        REVERSE
#
#
```

Laboratório - Módulo 9

```
┌──(root💀kali)-[~]
└─# scalpel /dev/sdb6 -o /mnt/teste4

Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.

Opening target "/dev/sdb6"

Image file pass 1/2.
/dev/sdb6: 100.0% |*****************************************************************************************************|  873.0 MB    00:00 ETA
Allocating work queues ...
Work queues allocation complete. Building carve lists ...
Carve lists built.  Workload:
jpg with header "\xff\xd8\xff\x3f\x3f\x3f\x45\x78\x69\x66" and footer "\xff\xd9" --> 0 files
jpg with header "\xff\xd8\xff\x3f\x3f\x3f\x4a\x46\x49\x46" and footer "\xff\xd9" --> 14 files
Carving files from image.
Image file pass 2/2.
/dev/sdb6: 100.0% |*****************************************************************************************************|  873.0 MB    00:00 ETA
Processing of image file complete. Cleaning up ...
Done.
Scalpel is done, files carved = 14, elapsed = 3 seconds.

┌──(root💀kali)-[~]
└─# ls /mnt/teste4/jpg-1-0/*
/mnt/teste4/jpg-1-0/00000000.jpg  /mnt/teste4/jpg-1-0/00000004.jpg  /mnt/teste4/jpg-1-0/00000008.jpg  /mnt/teste4/jpg-1-0/00000012.jpg
/mnt/teste4/jpg-1-0/00000001.jpg  /mnt/teste4/jpg-1-0/00000005.jpg  /mnt/teste4/jpg-1-0/00000009.jpg  /mnt/teste4/jpg-1-0/00000013.jpg
/mnt/teste4/jpg-1-0/00000002.jpg  /mnt/teste4/jpg-1-0/00000006.jpg  /mnt/teste4/jpg-1-0/00000010.jpg
/mnt/teste4/jpg-1-0/00000003.jpg  /mnt/teste4/jpg-1-0/00000007.jpg  /mnt/teste4/jpg-1-0/00000011.jpg
```

Laboratório - Módulo 9

Questão 9.3 - Execute o PhotoRec sobre **a área livre (free)** do volume sdb6, salvando os arquivos recuperados em "/mnt/teste5". Quantos arquivos de imagem do tipo ".jpg" foram recuperados?

1

Laboratório - Módulo 9

Questão 9.4 - Execute o PhotoRec sobre **todo o disco (whole)** do volume sdb6, salvando os arquivos recuperados em "/mnt/teste6". Quantos arquivos de imagem do tipo ".jpg" foram recuperados?

11

Laboratório - Módulo 9

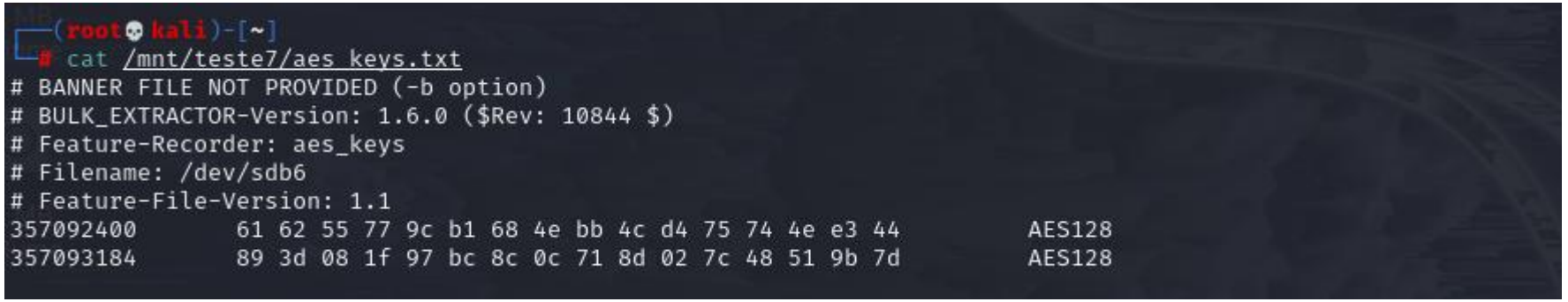
Questão 9.5 - Execute a ferramenta "bulk_extractor" sobre a pasta "/mnt/analise" (montada com o "/dev/sdb6") e salve o resultado em "/mnt/teste7". Quantas chaves AES foram recuperadas?

2

Laboratório - Módulo 9

```
┌──(root💀kali)-[~/plaso/tools]
└─# bulk_extractor /mnt/analise -R -o /root/bulk                                1 ⚙
mkdir "/root/bulk"
bulk_extractor version: 2.0.0-beta2
Input file: "/mnt/analise"
Output directory: "/root/bulk"
Disk Size: 25
Scanners: aes base64 elf evtx exif facebook find gzip httplogs json kml msxml net ntfsindx ntfslogfile ntfsmft ntfsusn pdf rar s
qlite utmp vcard windirs winlnk winpe winprefetch zip accts email gps
Threads: 2
going multi-threaded ... ( 2 )
bulk_extractor      Sun Nov 21 12:52:04 2021
```

Laboratório - Módulo 9



ANEXOS

LABORATÓRIO

Módulo 10

Estudo de caso: ferramentas de análise em sistemas Linux

Laboratório - Módulo 10

INSTRUÇÕES

1) Criar um arquivo de nome "teste10.txt" com conteúdo "1234" (echo 1234 > teste10.txt)
2) Gere um arquivo de listagem de hashes de nome "log_hash.txt" com o hash apenas desse arquivo (sha256sum teste10.txt > log_hash.txt)

Laboratório - Módulo 10

Questão 10.1 - Qual o hash SHA256 do arquivo "teste10.txt"?

SHA256:
a883dafc480d466ee04e0d6da986bd78eb1fdd2178d04693723da3a8f95d42f4

Laboratório - Módulo 10

Laboratório - Módulo 10

Questão 10.2 - Valide o arquivo de hashes "log_hash.txt". Ele é válido?

(**X**) SIM

( ) NÃO

Laboratório - Módulo 10

```
┌──(root💀kali)-[~]
└─# sha256sum -c log_hash.txt
teste10.txt: OK
```

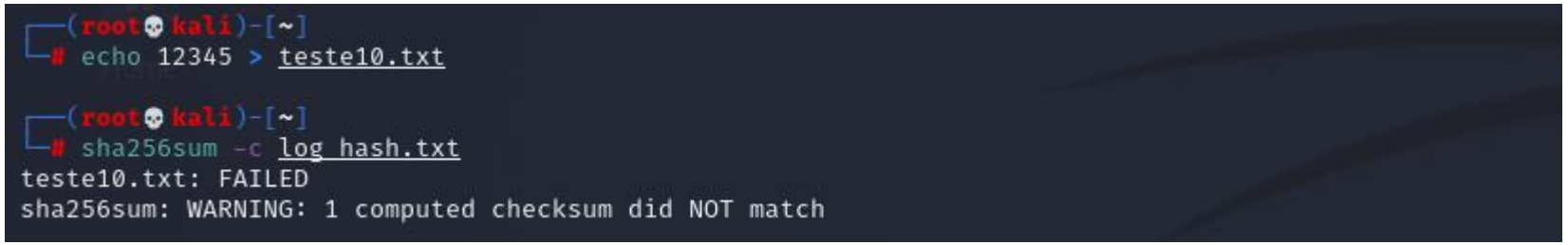
Laboratório - Módulo 10

Questão 9.3 - Execute o comando "echo 12345 > teste10.txt" e teste novamente. O arquivo de listagem de hashes continua válido?

( ) SIM

(**X**) NÃO

Laboratório - Módulo 10



Laboratório - Módulo 10

Questão 10.4 - Identifique o tipo de particionamento e o início (em setores) da segunda partição do arquivo de imagem "/mnt/analise/imagem2.dd":

(**X**) GPT / 63488

( ) MBR / 63488

( ) GPT / 2048

( ) MBR / 2048

Laboratório - Módulo 10

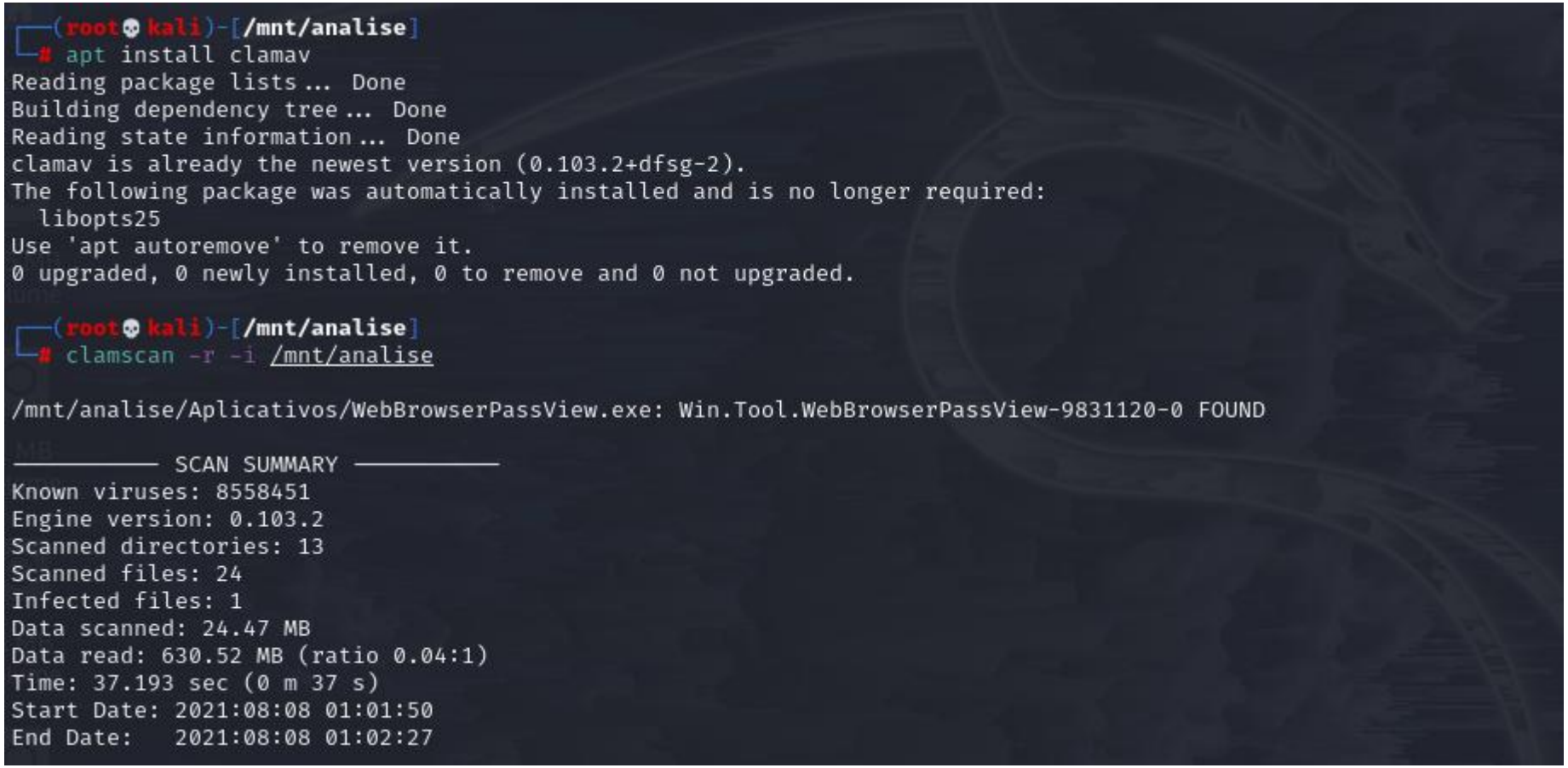
Laboratório - Módulo 10

Questão 10.5 - Instale e execute o antivírus "clamav" sobre a pasta "/mnt/analise". Foi encontrado algum malware?

(**X**) SIM. Nome do arquivo: **WebBrowserPassView.exe**

( ) NÃO

Laboratório - Módulo 10



LABORATÓRIO

Módulo 11

Arquivos de Log

Laboratório - Módulo 11

Questão 11.1 - Quais as duas primeiras palavras, após o horário, presentes na primeira linha do arquivo de log do kernel ("/dev/kmsg")? Uma dica é usar a ferramenta "dmesg".

Linux version

Laboratório - Módulo 11

```
┌──(root💀kali)-[~]
└─# dmesg | more
[    0.000000] Linux version 5.10.0-kali9-amd64 (devel@kali.org) (gcc-10 (Debian 10.2.1-6) 10.2.1 20210110, GNU ld (GNU Binutils for Debian) 2.35.2)
#1 SMP Debian 5.10.46-1kali1 (2021-06-25)
[    0.000000] Command line: BOOT_IMAGE=/boot/vmlinuz-5.10.0-kali9-amd64 root=UUID=dff30eeb-7332-438d-964c-d5c7f4d357f7 ro quiet splash
[    0.000000] x86/fpu: x87 FPU will use FXSAVE
[    0.000000] BIOS-provided physical RAM map:
[    0.000000] BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
[    0.000000] BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
[    0.000000] BIOS-e820: [mem 0x0000000000100000-0x000000007ffeffff] usable
[    0.000000] BIOS-e820: [mem 0x000000007fff0000-0x000000007fffffff] ACPI data
[    0.000000] BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
[    0.000000] NX (Execute Disable) protection: active
```

Laboratório - Módulo 11

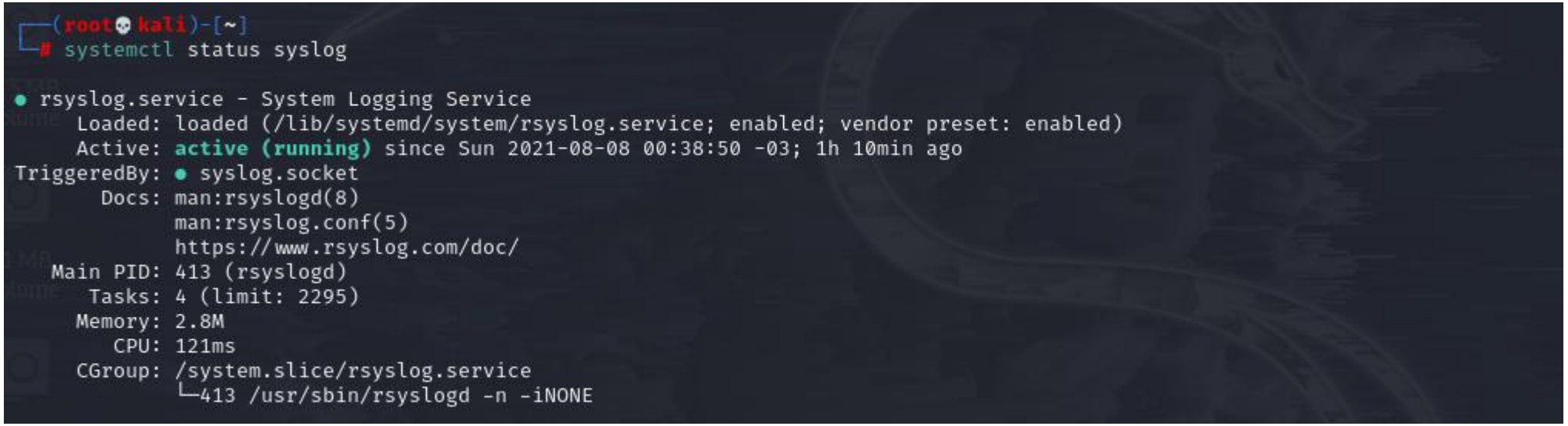
Questão 11.2 - O serviço "syslog" está em execução (ativo)? Qual comando utilizado para identificar isso?

(**X**) SIM

( ) NÃO

Comando: **systemctl status syslog**

Laboratório - Módulo 11

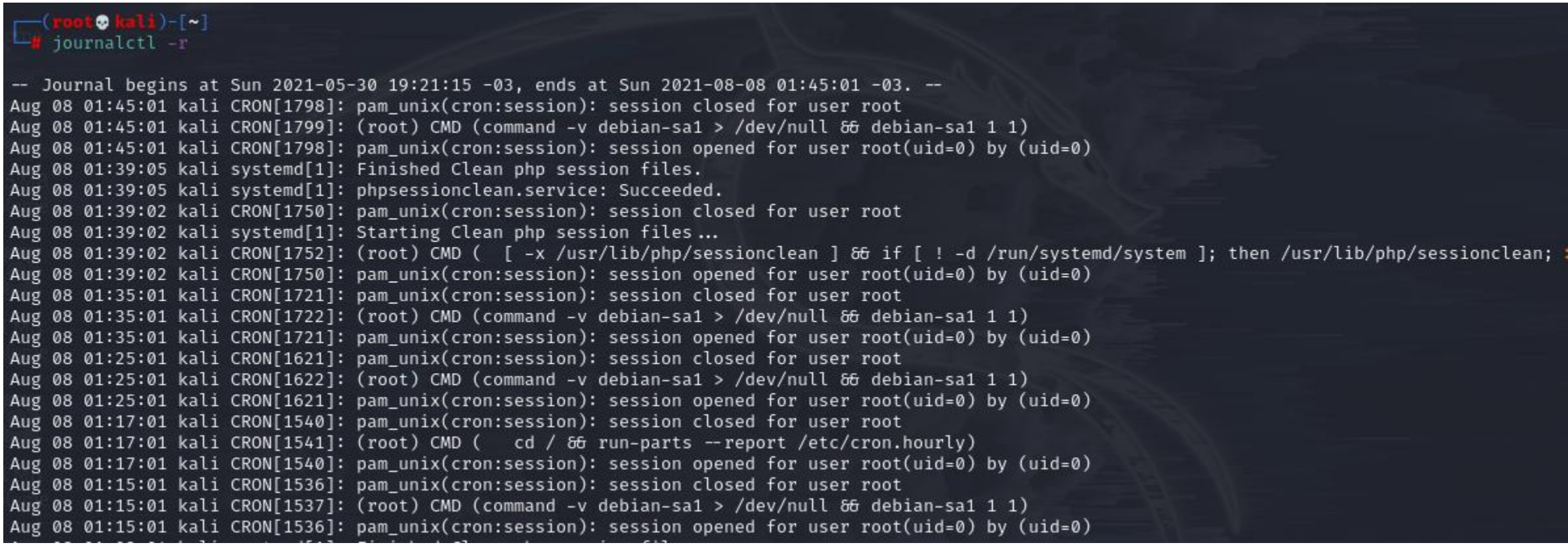


Laboratório - Módulo 11

Questão 11.3 - Qual o comando para recuperar os últimos registros do systemd-journal?

journalctl -r

Laboratório - Módulo 11



Laboratório - Módulo 11

Questão 11.4 - Quantas semanas são salvas por padrão no logrotate?

( ) 1

( ) 2

( ) 3

(**X**) 4

Laboratório - Módulo 11

```
┌──(root💀kali)-[~]
└─# cat cat /etc/logrotate.conf

cat: cat: No such file or directory
# see "man logrotate" for details

# global options do not affect preceding include directives

# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# use date as a suffix of the rotated file
#dateext

# uncomment this if you want your log files compressed
#compress

# packages drop log rotation information into this directory
include /etc/logrotate.d

# system-specific logs may also be configured here.
```

LABORATÓRIO

Módulo 12
Outras fontes de informação em sistemas Linux

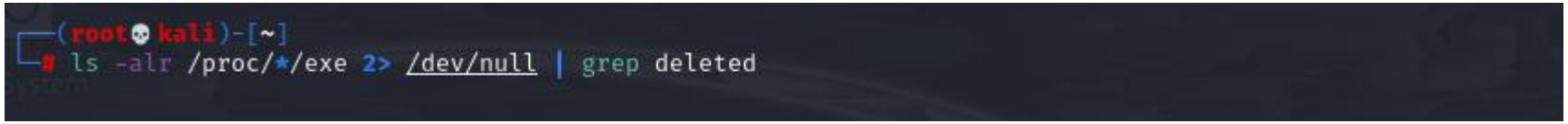
Laboratório - Módulo 12

Questão 12.1 - Existe algum aplicativo em execução que tenha sido apagado?

( ) SIM

(**X**) NÃO

Laboratório - Módulo 12



Laboratório - Módulo 12

Questão 12.2 - O arquivo "/etc/rc.local" é executado no Kali? Qual comando utilizado para comprovar isso?

( ) SIM

(**X**) NÃO

Comando: **systemctl status rc-local**

Laboratório - Módulo 12

Laboratório - Módulo 12

Questão 12.3 - Qual arquivo de shell do usuário root é executado (com o nome da pasta) quando é aberto um terminal, considerando o uso do shell zsh?

/root/.zshrc

Laboratório - Módulo 12

Questão 12.4 - Onde está localizado e qual o nome do arquivo de histórico de comandos do usuário "kali", considerando que ele usa o shell zsh?

/home/kali/.zsh_history

Laboratório - Módulo 12

Questão 12.5 - Existe um usuário com nome "postgres" habilitado? Com qual comando isso foi identificado?

(**X**) SIM

( ) NÃO

Comando: **cat /etc/passwd | grep postgres**

LABORATÓRIO

Módulo 13
Estudo de
Vulnerabilidades

Laboratório - Módulo 13

Questão 13.1 - Não existem vulnerabilidades de segurança no Sistema Operacional Linux:

( ) VERDADEIRO

(**X**) FALSO

Laboratório - Módulo 13

Questão 13.2 - São ferramentas que podem ser utilizadas para validação da segurança de computadores:

( ) Lynis

( ) Nikto

( ) nmap

( ) unix-privesc-check

(X) Todos anteriores

Laboratório - Módulo 13

Questão 13.3 - Qual é a ferramenta muito utilizada em testes de vulnerabilidades que utiliza diversas técnicas para identificar serviços sendo executados em determinadas portas?

( ) Lynis

( ) Nikto

(**X**) nmap

( ) unix-privesc-check

Laboratório - Módulo 13

Questão 13.4 - Ferramenta utilizada para validar uma série de serviços e configurações de um computador com Linux, para validar compliance e hardening?

(**X**) Lynis

( ) Nikto

( ) nmap

( ) unix-privesc-check

Laboratório - Módulo 13

Questão 13.5 - Ferramenta utilizada para validar a existência de vulnerabilidades específicas para escalamento de privilégios?

( ) Lynis

( ) Nikto

( ) nmap

(**X**) unix-privesc-check

IPOG INSTITUTO DE PÓS-GRADUAÇÃO & GRADUAÇÃO

Inspirando vidas.

www.ipog.edu.br

facebook.com/ipogbrasil
@ipogbrasil
@ipogbrasil
youtube.com/ipogbrasil
linkedin.com/school/ipogbrasil
blog.ipog.edu.br