

# Born2beRoot

Este projeto consiste em configurar um servidor, em que:

- Instale sistema operacional;

- Particionar discos com LVM;

- Crie conexão ssh;

- Instale firewall;

- Crie usuários e grupos;

- Crie regras para o sudo;

- Crie política de senhas;

- Agende com cron;

- Execute um scrip com informações da rede e do sistema.

# Servidores

Os servidores surgiram diante da necessidade de ter computadores de rede para usos específicos, principalmente para oferecer serviços de forma centralizada.

Dessa forma torna-se desnecessária, por exemplo, a instalação de uma ferramenta em cada máquina de uma empresa — basta que ela seja executado no servidor e os diversos computadores estejam conectados em rede com ele para que possam obter os resultados.

Os servidores processam e executam solicitações feitas por usuário através de softwares, bancos de dados, envio e recebimento de informações como e-mails, envio de formulários, hospedagem de websites e outros.

Um servidor funciona, grosso modo, como um grande computador, mas ao invés de executar operações em nível doméstico, ele o faz em grande escala, transferindo esses resultados para diferentes computadores.

Alguns exemplos de uso de servidores podem ser:

- hospedagem de internet;
- armazenamento de arquivo local;
- fornecimento de aplicações ERP para a organização;
- serviços de e-mail;
- serviço de bancos de dados;
- sistemas de pagamentos;
- aplicações de telefonia;
- uso de Internet das Coisas (Internet of Things ou IoT), entre outros.

Um servidor serve para centralizar grandes operações virtuais em um único "computador", trazendo mais desempenho para a execução de determinadas tarefas.

Quando uma empresa precisa, por exemplo, de uma ferramenta específica para executar uma tarefa, um servidor torna desnecessária a instalação desta ferramentas em cada uma das máquinas que precisarão utilizá-la: basta tê-la instalada em um servidor a que todos estes computadores estejam conectados.

# Virtualização

## General guidelines

- The use of VirtualBox (or UTM if you can't use VirtualBox) is mandatory.
- You only have to turn in a `signature.txt` file at the root of your repository. You must paste in it the signature of your machine's virtual disk. Go to Submission and peer-evaluation for more information.

**VirtualBox** é um produto de virtualização da Oracle para expandir os recursos de utilização do seu computador.

Mas, o que é virtualização? Virtualização trata-se da criação de um ou mais ambientes **virtuais** dentro de um mesmo computador físico, que funcionam de maneiras independentes.

Isso significa que neste mesmo computador, você pode ter várias "máquinas" diferentes, com sistemas operacionais, armazenamento, rede e programas distintos do hardware original.

Este processo é o que ocorre em servidores de hospedagem de sites ou no armazenamento em nuvem, por exemplo.

Para sua utilização, é necessário baixar e instalar o aplicativo diretamente da plataforma Oracle, então, é executado em uma janela à parte, como qualquer aplicativo, por isso não danifica ou faz qualquer alteração no seu computador. Assim, ao finalizar sua utilização basta fechar essa janela e operar o dispositivo normalmente.

A utilização do VirtualBox para executar vários sistemas operacionais em um mesmo computador já é um enorme benefício, que ainda se ramifica em diversas outras vantagens, como:

- Reduz custos de aquisição de diferentes hardwares e pode ser utilizado gratuitamente;
- Reduz custos com eletricidade e otimiza espaço, uma vez que apenas um computador por usuário pode ficar ligado;
- Reduz custos com servidores externos, já que você pode criar seu próprio servidor;
- Pode-se utilizar até mesmo sistemas operacionais mais antigos, sem preocupação com a compatibilidade do seu hardware;
- Não é necessário reiniciar o hardware para alternar entre sistemas operacionais, o que consequentemente aumenta a produtividade do usuário;
- Os desenvolvedores podem fazer diversos testes em uma única máquina;
- A segurança de cada máquina virtual é independente, sendo assim, caso uma delas sofra algum dano, as outras não serão impactadas.

# Sistema Operacional

You must choose as an operating system either the latest stable version of Debian (no testing/unstable), or the latest stable version of CentOS. Debian is highly recommended if you are new to system administration.



Debian, anteriormente chamado Debian GNU/Linux e hoje apenas Debian, é um sistema operacional composto inteiramente de software livre e mantido oficialmente pelo Projeto Debian. O projeto recebe, ainda, apoio de outros indivíduos e organizações de todo o mundo.

Curiosidade: o Ubuntu é um sistema operacional de código aberto, construído a partir do núcleo Linux, baseado no Debian e utiliza GNOME como ambiente de desktop de sua mais recente versão com suporte de longo prazo.

# Partições Criptografadas

Você deve criar pelo menos 2 partições criptografadas usando o LVM. Abaixo segue um exemplo de particionamento esperado:

You must create at least 2 encrypted partitions using LVM. Below is an example of the expected partitioning:

```
wil@wil:~$ lsblk
NAME                                MAJ:MIN RM  SIZE RO TYPE  MOUNTPOINT
sda                                  8:0      0   8G  0 disk
├─sda1                              8:1      0 487M  0 part  /boot
├─sda2                              8:2      0    1K  0 part
├─sda5                              8:5      0  7.5G  0 part
│   └─sda5_crypt                    254:0     0  7.5G  0 crypt
│       ├─wil--vg-root               254:1     0  2.8G  0 lvm    /
│       ├─wil--vg-swap_1             254:2     0  976M  0 lvm    [SWAP]
│       └─wil--vg-home               254:3     0  3.8G  0 lvm    /home
sr0                                  11:0     1 1024M  0 rom
wil@wil:~$ _
```

Feito na instalação do Debian. A verificação foi feita pelo comando lsblk.

Você pode pensar em LVM como "partições dinâmicas", o que significa que você pode criar/redimensionar/excluir "partições" LVM (elas são chamadas de "Volumes Lógicos" em LVM-speak) a partir da linha de comando *enquanto seu sistema Linux está em execução*: não precisa reinicializar o sistema para tornar o kernel ciente das partições recém-criadas ou redimensionadas.

Outros recursos interessantes que os "Volumes Lógicos" do LVM fornecem são:

1. Se você tiver mais de um disco rígido, os Volumes Lógicos podem se estender por mais de um disco: ou seja, eles não são limitados pelo tamanho de um único disco, mas pelo tamanho total agregado.
2. Você pode configurar LVs "distribuídos", para que a E/S possa ser distribuída para todos os discos que hospedam o LV em paralelo. (Semelhante ao RAID-0, mas um pouco mais fácil de configurar.)
3. Você pode criar um instantâneo (somente leitura) de qualquer LV. Você pode reverter o LV original para o instantâneo posteriormente ou excluir o instantâneo se não precisar mais dele. Isso é útil para backups de servidor, por exemplo (você não pode impedir que todos os seus aplicativos sejam gravados, então você cria um instantâneo e faz backup do instantâneo LV), mas também pode ser usado para fornecer uma "rede de segurança" antes de uma atualização crítica do sistema (clone o partição root, atualizar, reverter se algo der errado).

Embora seja mais útil em sistemas de servidor, acho que os recursos 1. e 3., combinados com a capacidade do LVM de criar/redimensionar/excluir LVs em tempo real, também são bastante úteis em sistemas de desktop. (Especialmente se você experimentar muito com o sistema.)

### **Desvantagens**

Claro, tudo isso tem um preço: a configuração inicial do LVM é mais complexa do que apenas particionar um disco, e você definitivamente precisará entender a terminologia e o modelo do LVM (Volumes Lógicos, Volumes Físicos, Grupos de Volume) antes de poder *começar* a usá-lo. (Uma vez configurado, é muito mais fácil usá-lo.)

Além disso, se você usar o LVM em discos rígidos, poderá perder todos os seus dados quando apenas uma unidade falhar.

# Ferramentas para instalação/remoção



During the defense, you will be asked a few questions about the operating system you chose. For instance, you should know the differences between aptitude and apt, or what SELinux or AppArmor is. In short, understand what you use!

○ APT foi projetado para lidar com a instalação e remoção de software. **○ APT faz parte do pacote .deb do Debian;** no entanto, ele foi atualizado para funcionar com o Gerenciador de Pacotes RPM.

○ APT é uma ferramenta de linha de comando. Isso significa que você precisa usar comandos para trabalhar com ele sem nenhuma referência visual de uma interface gráfica (o plano inicial era incluir uma interface gráfica, mas a ideia foi abandonada posteriormente). Para usá-lo, você precisa fornecer o nome do pacote. O pacote deve ter suas fontes especificadas em '/etc/apt/sources.list.' Ele também deve conter toda a lista de dependências que o pacote precisa para instalar automaticamente.

A abordagem adotada pela APT é flexível. Isso significa que o usuário pode configurar como o APT funciona, incluindo adicionar novas fontes, fornecer opções de atualização e assim por diante!

○ Aptitude também é uma ferramenta de empacotamento avançada. No entanto, é uma ferramenta de front-end que fornece aos usuários acesso à interface do usuário para acessar a funcionalidade. Isso significa que você pode usar o Aptitude para instalar e remover pacotes usando-o. ○ Debian criou o aptitude. Mas, com o tempo, eles o lançaram para outras distribuições baseadas em RPM.

Você pode instalá-lo usando o comando: **sudo apt install aptitude**

○ Aptitude pode ser usado para mais funcionalidades, incluindo pesquisa de pacotes, configuração de instalação de pacotes como automação ou manual e ações mais refinadas nos pacotes.

# Controle de acesso

**Security-Enhanced Linux (SELinux)** é uma arquitetura de segurança para [sistemas Linux®](#) que permite aos administradores mais controle sobre quem pode acessar o sistema. Ele foi originalmente desenvolvido pela Agência de Segurança Nacional (NSA) dos Estados Unidos como uma série de patches para o [kernel do Linux](#) usando módulos de segurança do Linux (LSM).

O SELinux define controles de acesso para aplicações, processos e arquivos em um sistema. Ele usa políticas de segurança, um conjunto de regras que dizem ao SELinux o que pode ou não ser acessado, para impor o acesso permitido por uma determinada política.

**AppArmor** é um sistema de *Controle de Acesso Mandatório* (MAC - Mandatory Access Control) construído sobre uma interface LSM ( *Linux Security Modules* ) do Linux. Na prática, o kernel consulta o AppArmor antes de cada chamada do sistema para saber se o processo está autorizado a fazer uma operação dada. Por meio desse mecanismo, o AppArmor confina programas a um conjunto de recursos limitados.

O AppArmor aplica um conjunto de regras (conhecidas como “perfil”) em cada programa. O perfil aplicado pelo kernel depende do caminho de instalação do programa que está sendo executado. Ao contrário do SELinux, as regras aplicadas não dependem do usuário. Todos os usuários enfrentam o mesmo conjunto de regras quando executam o mesmo programa (mas as permissões de usuário tradicionais ainda se aplicam e podem resultar em comportamentos diferentes!).

Os perfis do AppArmor são mantidos em uso `/etc/apparmor.d/` e contêm uma lista de controle de acesso em recursos que cada programa tem. Os perfis são compilados e carregados no núcleo pelo comando **apparmor\_parser**. Cada perfil pode ser carregado tanto em modo de aplicação (“complaining”) quanto em modo de registro (“complaining”). O primeiro aplica a política e os relatórios de tentativas de sistema que foram mantidos negados enquanto não foram aplicados a políticas mas foram mantidos como negados.



### 14.4.2. Habilitando o AppArmor e gerenciando os perfis AppArmor

O suporte do AppArmor está embutido nos kernels padrão fornecidos pelo Debian. Ativar o AppArmor é, portanto, apenas uma questão de instalar alguns pacotes executando `apt install apparmor apparmor-profiles apparmor-utils` com privilégios de root.

O AppArmor está funcional após a instalação e `aa-status` confirmará rapidamente:

```
# aa-status
apparmor module is loaded.
40 profiles are loaded.
23 profiles are in enforce mode.
  /usr/bin/evince
  /usr/bin/evince-previewer
[...]
17 profiles are in complain mode.
  /usr/sbin/dnsmasq
[...]
14 processes have profiles defined.
12 processes are in enforce mode.
  /usr/bin/evince (3462)
[...]
2 processes are in complain mode.
  /usr/sbin/avahi-daemon (429) avahi-daemon
  /usr/sbin/avahi-daemon (511) avahi-daemon
0 processes are unconfined but have a profile defined.
```

#### NOTA Mais perfis AppArmor

O pacote `apparmor-profiles` contém perfis gerenciados pela comunidade upstream do AppArmor. Para obter ainda mais perfis você pode instalar o `apparmor-profiles-extra` que contém aprofundado pelo Ubuntu e Debian.

A SSH service will be running on port 4242 only. For security reasons, it must not be possible to connect using SSH as root.



The use of SSH will be tested during the defense by setting up a new account. You must therefore understand how it works.

Para desabilitar o acesso ao root e mudar a porta para 4242 é preciso editar o arquivo `/etc/ssh/sshd_config`.  
Comando usado:  
`nano /etc/ssh/sshd_config`

**Secure Socket Shell** é um protocolo de rede que oferece aos usuários, principalmente aos administradores de sistema, uma maneira segura de acessar um computador em uma rede não segura. Ele fornece aos usuários uma autenticação de senha forte, bem como uma autenticação de chave pública. Ele tenta comunicar com segurança dados criptografados em dois computadores usando uma rede aberta.

Este número de porta é frequentemente usado como uma porta de exemplo em demonstrações de código ou como uma porta HTTP alternativa. A razão pela qual isso é tão popular é porque repete o número 42, um número popular entre os geeks de computador. No livro clássico de Douglas Adams "Hitch Hikers Guide to the Galaxy", o número "42" é a resposta para a vida, o universo e tudo mais.

Deve remover `apache2` e mudar o IP para estático para ficar igual ao subject.

```
root@jvidon-n42:~# ss -tunlp
Netid      State      Recv-Q     Send-Q      Local Address:Port      Peer Address:Port
Process
udp        UNCONN     0           0            0.0.0.0:68              0.0.0.0:*
users: (('dhclient',pid=517,fd=9))
tcp        LISTEN     0           128          0.0.0.0:4242            0.0.0.0:*
users: (('sshd',pid=572,fd=3))
tcp        LISTEN     0           511          *:80                  *:
users: (('apache2',pid=576,fd=4), ('apache2',pid=575,fd=4), ('apache2',pid=573,fd=4))
tcp        LISTEN     0           128          [::]:4242             [::]:*
users: (('sshd',pid=572,fd=4))
root@jvidon-n42:~# _
```

```
#Port 4242
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin no
```

You have to configure your operating system with the UFW firewall and thus leave only port 4242 open.



Your firewall must be active when you launch your virtual machine.  
For CentOS, you have to use UFW instead of the default firewall. To install it, you will probably need DNF.

```
root@jvidon-n42:/# sudo ufw status verbose
Status: inactive
root@jvidon-n42:/# sudo ufw enable
Firewall is active and enabled on system startup
root@jvidon-n42:/# sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
root@jvidon-n42:/# sudo ufw allow 4242
Rule added
Rule added (v6)
root@jvidon-n42:/# sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To               Action       From
--
4242             ALLOW IN    Anywhere
4242 (v6)        ALLOW IN    Anywhere (v6)

root@jvidon-n42:/#
```

- You have to implement a strong password policy.

To set up a strong password policy, you have to comply with the following requirements:

- Your password has to expire every 30 days.
- The minimum number of days allowed before the modification of a password will be set to 2.
- The user has to receive a warning message 7 days before their password expires.
- Your password must be at least 10 characters long. It must contain an uppercase letter, a lowercase letter, and a number. Also, it must not contain more than 3 consecutive identical characters.
- The password must not include the name of the user.
- The following rule does not apply to the root password: The password must have at least 7 characters that are not part of the former password.
- Of course, your root password has to comply with this policy.

```
# Password aging controls:
#
#     PASS_MAX_DAYS   Maximum number of days a password may be used.
#     PASS_MIN_DAYS   Minimum number of days allowed between password changes.
#     PASS_WARN_AGE   Number of days warning given before a password expires.
#
PASS_MAX_DAYS 30
PASS_MIN_DAYS 2
PASS_WARN_AGE 7
```



After setting up your configuration files, you will have to change all the passwords of the accounts present on the virtual machine, including the root account.

<https://www.networkworld.com/article/2726217/how-to-enforce-password-complexity-on-linux.html>

hostnamectl set-hostname user

- The **hostname** of your virtual machine must be your login ending with 42 (e.g., wil42). You will have to modify this hostname during your evaluation.

```
root@jvidon-n42:~# chage -M 30 jvidon-n
root@jvidon-n42:~# chage -M 30 root
root@jvidon-n42:~# chage -m 2 jvidon-n
root@jvidon-n42:~# chage -m 2 root
```

```
root@jvidon-n42:~# chage -l jvidon-n
Última mudança de senha          : jun 02, 2022
Senha expira                     : jul 02, 2022
Senha inativa                    : nunca
Conta expira                     : nunca
Número mínimo de dias entre troca de senhas : 2
Número máximo de dias entre troca de senhas : 30
Número de dias de avisos antes da expiração da senha : 7
root@jvidon-n42:~# chage -l root
Última mudança de senha          : jun 02, 2022
Senha expira                     : jul 02, 2022
Senha inativa                    : nunca
Conta expira                     : nunca
Número mínimo de dias entre troca de senhas : 2
Número máximo de dias entre troca de senhas : 30
Número de dias de avisos antes da expiração da senha : 7
root@jvidon-n42:~#
```

```
root@jvidon-n42:~# passwd jvidon-n
Nova senha:
Redigite a nova senha:
passwd: senha atualizada com sucesso
root@jvidon-n42:~# passwd root
Nova senha:
SENHA INCORRETA: A senha contém menos do que 1 dígitos
Nova senha:
SENHA INCORRETA: A senha contém menos do que 1 dígitos
Nova senha:
Redigite a nova senha:
passwd: senha atualizada com sucesso
root@jvidon-n42:~#
```

O **sudo** é um utilitário de linha de comando para permitir usuários normais a executarem outros utilitários com permissões mais elevadas, de acordo com as suas regras. Ou seja, o sudo controla os acessos dos usuários normais ao super-usuário do sistema, também conhecido como root.

O **su** é apenas um comando para trocar de usuário. O “s” significa “switch” e o “u” significa “user”, isto é, “switch user” (trocar de usuário). O objetivo de colocar o “sudo” como antecedente, é porque o “su” já vai ser executado como super-usuário, trocando o usuário da sessão atual para o “root”.

\$ sudo su # Muda para o usuário root

\$ su mateus # Muda para o usuário mateus

A ideia do sudo é justamente ser o antecedente de cada comando para elevar a sua permissão.

Veja a diferença com sudo e sem sudo:

```
[vagrant@localhost ~]$ cat /etc/shadow
cat: /etc/shadow: Permission denied
[vagrant@localhost ~]$ sudo cat /etc/shadow
root:$1$QDyPlph/$oaAX/xNRf3aiW3l27NIUA/::0:99999:7:::
hin:*:17834:0:99999:7:::
```

Toda a configuração do utilitário sudo é feita no arquivo /etc/sudoers. Você pode ver o que está configurado com o comando:

\$ cat /etc/sudoers

- You have to install and configure `sudo` following strict rules.

To set up a strong configuration for your `sudo` group, you have to comply with the following requirements:

- Authentication using `sudo` has to be limited to 3 attempts in the event of an incorrect password.
- A custom message of your choice has to be displayed if an error due to a wrong password occurs when using `sudo`.
- Each action using `sudo` has to be archived, both inputs and outputs. The log file has to be saved in the `/var/log/sudo/` folder.
- The TTY mode has to be enabled for security reasons.
- For security reasons too, the paths that can be used by `sudo` must be restricted.  
Example:  
`/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin`

```
Defaults    env_reset
Defaults    mail_badpass
Defaults    secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin/snap/bin"
Defaults    passwd_tries=3
Defaults    badpass_message="login incorrect"
Defaults    requiretty
Defaults    logfile="/var/log/sudo/folder"
```

O `sudo` tem somente um arquivo de configuração, o `/etc/sudoers` que pode ser editado de duas formas, a primeira utilizando o seu editor de texto preferido (vi por exemplo) e a segunda forma é utilizando o comando `visudo`, que na verdade parece executar um `vi sudo`, só que além disto, o `visudo` previne que mais de uma pessoa edite o `sudoers` simultaneamente e contém algumas rotinas de verificação de sintaxe do arquivo. Então para editar o `sudoers`, utilize SEMPRE o `visudo`.

Comando usado:  
`sudo visudo -f etc/sudoers`

O diretório `/var` contém arquivos que aumentam de tamanho ao longo do tempo. Portanto, nada mais justo do que os arquivos de log do sistema também fiquem aqui, mais especificamente em `/var/log`.



During the defense, you will have to create a new user and assign it to a group.

- In addition to the root user, a user with your login as username has to be present.
- This user has to belong to the user42 and sudo groups.

```
root@jvidon-n42:~# groupadd user42
root@jvidon-n42:~# groupadd sudo
groupadd: grupo 'sudo' já existe
root@jvidon-n42:~# gpasswd -a jvidon-n sudo
Adicionando usuário jvidon-n ao grupo sudo
root@jvidon-n42:~# gpasswd -a jvidon-n user42
Adicionando usuário jvidon-n ao grupo user42
root@jvidon-n42:~# groups jvidon-n
jvidon-n : jvidon-n cdrom floppy sudo audio dip video plugdev netdev bluetooth user42
root@jvidon-n42:~# getent group sudo
sudo:x:27:jvidon-n
root@jvidon-n42:~# getent group user42
user42:x:1001:jvidon-n
root@jvidon-n42:~# id -g jvidon-n
1000
root@jvidon-n42:~#
```

useradd <username> - crie um novo usuário com o diretório inicial;

Para adicionar um usuário ao sudogruppo você deve usar o comando gpasswd -a <username> sudo.



Finally, you have to create a simple script called `monitoring.sh`. It must be developed in `bash`.

At server startup, the script will display some information (listed below) on all terminals every 10 minutes (take a look at `wall`). The banner is optional. No error must be visible.

Your script must always be able to display the following information:

- The architecture of your operating system and its kernel version.
- The number of physical processors.
- The number of virtual processors.
- The current available RAM on your server and its utilization rate as a percentage.
- The current available memory on your server and its utilization rate as a percentage.
- The current utilization rate of your processors as a percentage.
- The date and time of the last reboot.
- Whether LVM is active or not.
- The number of active connections.
- The number of users using the server.
- The number of users using the server.
- The IPv4 address of your server and its MAC (Media Access Control) address.
- The number of commands executed with the `sudo` program.

```
Server10 [Executando] - Oracle VM VirtualBox
Arquivo  Máquina  Visualizar  Entrada  Dispositivos  Ajuda
GNU nano 5.4                                monitoring.sh
#!/bin/bash

ARCHITECTURE=$(uname -a)
CPU=$(lscpu | sed -n '5p' | awk '{print $2}')
VIRTUALCPU=$(grep 'processor' /proc/cpuinfo | uniq | wc -l)
USAGERAM=$(free -m | sed -n '2p' | awk '{print $3}')
TOTALRAM=$(free -m | sed -n '2p' | awk '{print $2}')
PERC=$(free -m | sed -n '2p' | awk '{printf("%.2f"), $3/$2*100}')
DISKUSAGE=$(df -m --total | sed -n '10p' | awk '{print $3}')
DISKAVAILABLE=$(df -h --total | sed -n '10p' | awk '{print $4}')
CPUL=$(top -bn1 | grep '%Cpu' | cut -c 9- | xargs | awk '{printf("%.1f%%"), $1 + $3}')
PERCENTDISK=$(df -h --total | sed -n '10p' | awk '{print $5}')
LASTBOOT=$(who -b | awk '{print $4 " " $5}')
LVM=$(lsblk | grep "lvm" | wc -l)
CHECKLVM=$(if [ $LVM == 0 ]; then echo no; else echo yes; fi)
TCPCONNECTION=$(ss -s | sed -n '7p' | awk '{print $2}')
USERLOG=$(users | wc -w)
IPADDRESS=$(hostname -I)
MACADDRESS=$(ip link show | grep "ether" | awk '{print $2}')
SUDO=$(grep -c "COMMAND" /var/log/sudo/folder)

wall "

#Architecture: $ARCHITECTURE
#CPU physical : $CPU
#vCPU : $VIRTUALCPU
#Memory Usage: ${USAGERAM}/${TOTALRAM}MB (${PERC}%)
#Disk Usage: $DISKUSAGE/$DISKAVAILABLE ($PERCENTDISK)
#CPU load: $CPUL
#Last boot: $LASTBOOT
#LVM use: $CHECKLVM
#Connections TCP : $TCPCONNECTION ESTABLISHED
#User log: $USERLOG
#Network: IP $IPADDRESS($MACADDRESS)

[ 35 linhas lidas ]
^G Ajuda  ^O Gravar  ^W Onde está? ^K Recortar  ^T Executar  ^C Local  M-U Desfazer
^X Sair    ^R Ler o arq ^\ Substituir ^U Colar    ^J Justificar ^_ Ir p/ linha M-E Refazer
```

```
jvidon-n42: # bash monitoring.sh
gem de broadcast de root@jvidon-n42 (tty1) (Sat Jun  4 20:26:05 2022):

#Architecture: Linux jvidon-n42 5.10.0-14-amd64 #1 SMP Debian 5.10.113-1 (2022-04-29) x86_64
Linux
#CPU physical : 18%
#vCPU : 1
#Memory Usage: 80/976MB (8,20%)
#Disk Usage: 1583/6,0G (21%)
#CPU load: 18%
#Last boot: 2022-06-04 20:24
#LVM use: yes
#Connections TCP : 3 ESTABLISHED
#User log: 1
#Network: IP 10.0.2.15 (08:00:27:06:1c:19)
#Sudo : 18 cmd
```

```

ARCHITECTURE=$(uname -a)
CPU=$(lscpu | sed -n '5p' | awk '{print $2}')
VIRTUALCPU=$(grep 'processor' /proc/cpuinfo | uniq | wc -l)
USAGERAM=$(free -m | sed -n '2p' | awk '{print $3}')
TOTALRAM=$(free -m | sed -n '2p' | awk '{print $2}')
PERC=$(free -m | sed -n '2p' | awk '{printf("%.2f"), $3/$2*100}')

```

Retorna o nome e versão do kernel atual

- a, -all (imprime toda informação)

**Número de processadores físicos:** lscpu reúne informações de arquitetura de CPU e sed -n serve para filtrar o texto, mostra apenas a linha 2

**Número de processadores virtuais:**

Grep: pesquisa num arquivo e imprime as linhas correspondentes.

Uniq: Filtra linhas correspondentes

Wc - l: imprime contagens de nova linha

**Informações da memória:**

df - relata o uso do espaço em disco do sistema de arquivos.

-h para impressão em GB;

--total

**Utilização do CPU:**

top - exibe os processos do Linux

cut - remove seções de cada linha de arquivos (-c seleciona apenas 9 caracteres)

xargs - lê itens da entrada padrão, limitados por espaços em branco (que podem ser protegido com aspas duplas ou simples ou uma barra invertida) ou newlines e executa o comando (o padrão é echo ) um ou mais vezes com quaisquer argumentos iniciais seguidos por itens lidos de entrada padrão.

**Informações da memória RAM:**

Free -m (m para MB)

```

DISKUSAGE=$(df -m --total | sed -n '10p' | awk '{print $3}')
DISKAVAILABLE=$(df -h --total | sed -n '10p' | awk '{print $4}')
PERCENTDISK=$(df -h --total | sed -n '10p' | awk '{print $5}')
CPU=$(top -bn1 | grep '^%Cpu' | cut -c 9- | xargs | awk '{printf("%1.f%%"), $1 + $3}')

```

**Data e horário do último reboot:**

O comando who exibe informações de usuários "logados" no sistema, com a opção "b" podemos saber a data e o horário que o usuário logou no sistema, awk serve para imprimir as informações das colunas 4 e 5.

**Se LMV está ativo:** Este comando exibe informações sobre as partições do HD e outros dispositivos de armazenamento.

**Número de conexões ativas:** ss para informações sobre a rede (-s para estatísticas)

```

LASTBOOT=$(who -b | awk '{print $4 " " $5}')
LVM=$(lsblk | grep "lvm" | wc -l)
CHECKLVM=$(if [ $LVM == 0 ]; then echo no; else echo yes; fi)
TCPCONNECTION=$(ss -s | sed -n '7p' | awk '{print $2}')
NUSERLOG=$(users | wc -w)
IPADDRESS=$(hostname -I)
MACADDRESS=$(ip link show | grep "ether" | awk '{print $2}')
SUDO=$(grep -c "COMMAND" /var/log/sudo/folder)

```



During the defense, you will be asked to explain how this script works. You will also have to interrupt it without modifying it. Take a look at cron.

This is an example of how the script is expected to work:

```
Broadcast message from root@wil (tty1) (Sun Apr 25 15:45:00 2021):
```

```
#Architecture: Linux wil 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64 GNU/Linux
#CPU physical : 1
#vCPU : 1
#Memory Usage: 74/987MB (7.50%)
#Disk Usage: 1009/2Gb (39%)
#CPU load: 6.7%
#Last boot: 2021-04-25 14:45
#LVM use: yes
#Connections TCP : 1 ESTABLISHED
#User log: 1
#Network: IP 10.0.2.15 (08:00:27:51:9b:a5)
#Sudo : 42 cmd
```

```
* /10 * * * *
```

```
/home/user/script.sh
```

Para executar uma tarefa cron para o arquivo do script localizado no diretório home a cada 10 minutos.

```
crontab: installing new crontab
root@jvidon-n42:~# crontab -l
*/10 * * * * bash /home/user/monitoring.sh
root@jvidon-n42:~#
```

O **Cron** do **Linux** é um daemon que executa comandos ou scripts agendados por uma tabela chamada de **crontab**. A **configuração** do **cron** geralmente é chamada de **crontab**.

Para **configurar** um **crontab** por usuário, utiliza-se o comando “**crontab**”, junto com um parâmetro, dependendo do que você quiser fazer.

<https://www.vivaolinux.com.br/artigo/Como-executar-tarefas-a-cada-5-10-ou-15-minutos>

<https://www.hostinger.com.br/tutoriais/cron-job-guia#O-Que-e-Cron-Job>

<https://terminalroot.com.br/2014/12/como-utilizar-o-crontab.html>

TESTANDO

# Partições

```
Last login: Sat Jun  4 22:03:32 -03 2022 on tty1
root@jvidon-n42:~# lsblk
NAME                                MAJ:MIN RM  SIZE RO TYPE  MOUNTPOINT
sda                                  8:0    0   8G  0 disk
├─sda1                              8:1    0 487M  0 part  /boot
├─sda2                              8:2    0    1K  0 part
├─sda5                              8:5    0  7,5G  0 part
│   └─sda5_crypt                    254:0    0  7,5G  0 crypt
│       ├─jvidon--n42--vg-root       254:1    0  2,8G  0 lvm    /
│       ├─jvidon--n42--vg-swap_1     254:2    0  976M  0 lvm    [SWAP]
│       └─jvidon--n42--vg-home       254:3    0  3,7G  0 lvm    /home
sr0                                  11:0    1 1024M  0 rom
```

lsblk

# Configurações do sudo

```
# See the man page for details on how to write a sudoers file.
#
Defaults    env_reset
Defaults    mail_badpass
Defaults    secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin/snap/bin"
Defaults    passwd_tries=3
Defaults    badpass_message="login incorrect"
Defaults    requiretty
Defaults    logfile="/var/log/sudo/folder"
```

Sudo visudo /etc/sudoers

# App armor status

```
root@jvidon-n42:~# sudo aa-status
apparmor module is loaded.
6 profiles are loaded.
6 profiles are in enforce mode.
  /usr/bin/man
  lsb_release
  man_filter
  man_groff
  nvidia_modprobe
  nvidia_modprobe//kmod
0 profiles are in complain mode.
0 processes have profiles defined.
0 processes are in enforce mode.
0 processes are in complain mode.
0 processes are unconfined but have a profile defined.
root@jvidon-n42:~#
```

`sudo aa-status`

# Ufw status

```
root@jvidon-n42:~# ufw status
Status: active

To Action From
--
4242 ALLOW Anywhere
4242 (v6) ALLOW Anywhere (v6)

root@jvidon-n42:~# _
```

ufw status

Permitir nova porta:

`sudo ufw allow 8080`

Mostrar regras numeradas:

`sudo ufw status numbered`

Deletar regra:

`sudo ufw delete`

PS C:\Users\joana> ssh jvidon-n@192.168.0.161 -p 4242  
The authenticity of host '[192.168.0.161]:4242 ([192.168.0.161]:4242)' can't be established.  
ECDSA key fingerprint is SHA256:hNqwNdZJtmd3ka9rvaAmngKPFRG100fMzh39Lsis84c.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? y  
Please type 'yes', 'no' or the fingerprint: yes  
Warning: Permanently added '[192.168.0.161]:4242' (ECDSA) to the list of known hosts.  
jvidon-n@192.168.0.161's password:  
Linux joana 5.10.0-14-amd64 #1 SMP Debian 5.10.113-1 (2022-04-29) x86\_64

The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/\*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
Last login: Fri Jun 3 22:56:00 2022

Mensagem de broadcast de root@joana (somewhere) (Tue Jun 7 19:30:01 2022):

```
#Architecture: Linux joana 5.10.0-14-amd64 #1 SMP Debian 5.10.113-1 (2022-04-29) x86_64 GNU/Linux
#CPU physical : 1
#vCPU : 1
#Memory Usage: 73/976MB (7,48%)
#Disk Usage: 0/98M (0%)
#CPU load: 12%
#Last boot: 2022-06-07 19:27
#LVM use: yes
#Connections TCP : 3 ESTABLISHED
#User log: 2
#Network: IP 192.168.0.161 2804:14c:140:218b:a00:27ff:fe06:1c19 (08:00:27:06:1c:19)
#Sudo : 36 cmd
```

jvidon-n@joana:~\$

Para testar a conexão ssh  
do Windows para o  
servidor:

Windows + R  
Buscar por powershell

Comando:  
ssh user@IP -p 4242

Verificar se conexão está  
em Bridge



# Se as conexões estão como no subject

```
root@jvidon-n42:~# ss -tunlp
Netid State  Recv-Q  Send-Q  Local Address:Port  Peer Address:Port Process
tcp    LISTEN  0        128      0.0.0.0:4242      0.0.0.0:*    users:(("sshd",pid=581,fd=3))
tcp    LISTEN  0        128      [::]:4242       [::]:*      users:(("sshd",pid=581,fd=4))
root@jvidon-n42:~#
```

ss -tunlp

## hostname

- The `hostname` of your virtual machine must be your login ending with 42 (e.g., `wil42`). You will have to modify this hostname during your evaluation.

Hostnamedctl set-hostname  
novonome

## Política de senha

```
# here are the per-package modules (the "Primary" block)
password      requisite                                pam_pwquality.so retry=3 minlen=10 ucredit=-1 lcred
lcredit=-1 dcredit=-1 maxrepeat=3 reject_username difok=7 enforce_for_root
```

nano /etc/pam.d/common-password

```
root@jvidon-n42:~# chage -l root
Última mudança de senha          : jun 04, 2022
Senha expira                     : jul 04, 2022
Senha inativa                   : nunca
Conta expira                    : nunca
Número mínimo de dias entre troca de senhas : 2
Número máximo de dias entre troca de senhas : 30
Número de dias de avisos antes da expiração da senha : 7
root@jvidon-n42:~#
```

chage -l root

# Usuário e grupo

During the defense, you will have to create a new user and assign it to a group.

Adicionar usuário: `adduser nome`  
Adicionar grupo: `groupadd nome`  
Adicionar user ao grupo: `gpasswd -a usuário grupo`

- This user has to belong to the `user42` and `sudo` groups.

Verifica se usuário está no grupo:  
`getent group nome`

## Script

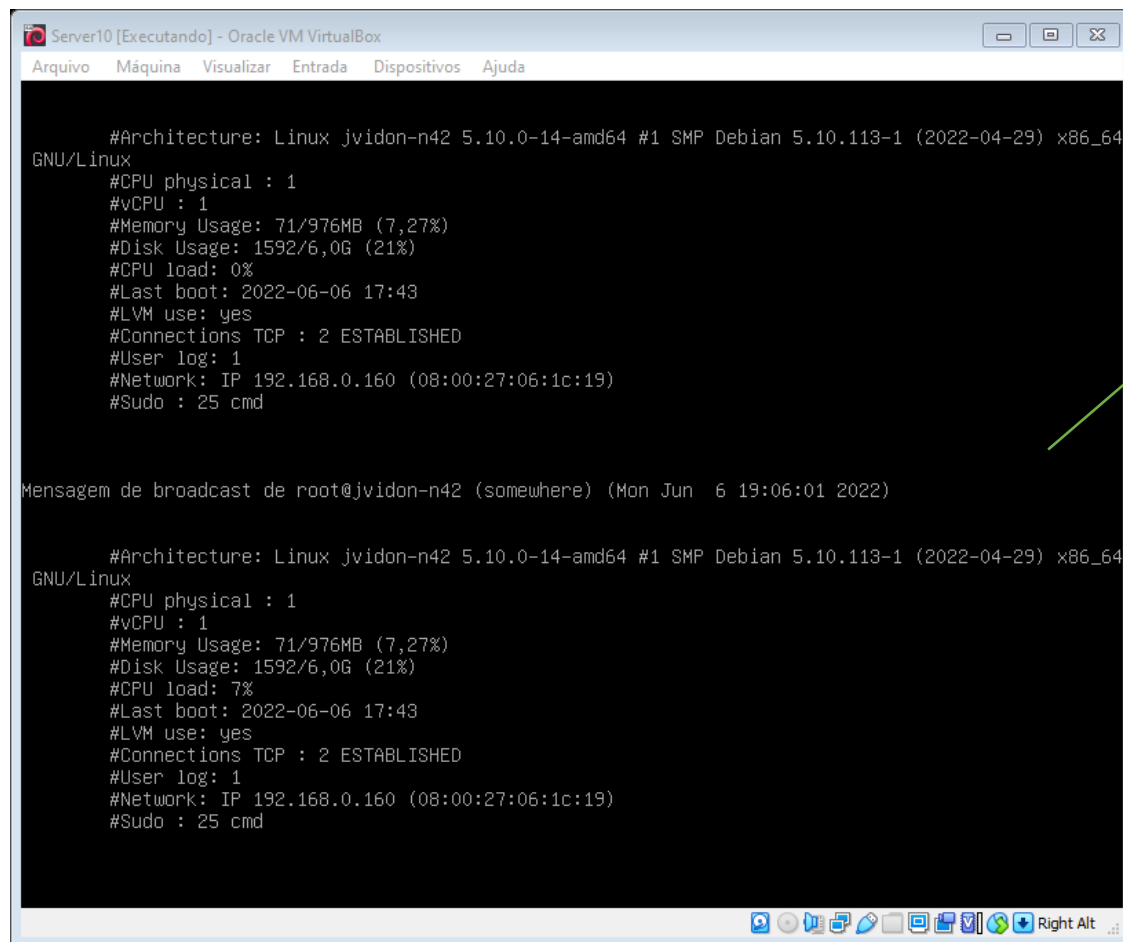
```
root@jvidon-n42:~# bash monitoring.sh
Mensagem de broadcast de root@jvidon-n42 (tty1) (Mon Jun  6 18:41:43 2022):

#Architecture: Linux jvidon-n42 5.10.0-14-amd64 #1 SMP Debian 5.10.113-1 (2022-04-29) x86_64
GNU/Linux
#CPU physical : 1
#vCPU : 1
#Memory Usage: 70/976MB (7,17%)
#Disk Usage: 1592/6,0G (21%)
#CPU load: 6%
#Last boot: 2022-06-06 17:43
#LVM use: yes
#Connections TCP : 2 ESTABLISHED
#User log: 1
#Network: IP 192.168.0.160 (08:00:27:06:1c:19)
#Sudo : 25 cmd

root@jvidon-n42:~#
```

# Cron

At server startup, the script will display some information (listed below) on all terminals every 10 minutes (take a look at `wall`). The banner is optional. No error must be visible.



```
Server10 [Executando] - Oracle VM VirtualBox
Arquivo  Máquina  Visualizar  Entrada  Dispositivos  Ajuda

#Architecture: Linux jvidon-n42 5.10.0-14-amd64 #1 SMP Debian 5.10.113-1 (2022-04-29) x86_64
GNU/Linux
#CPU physical : 1
#vCPU : 1
#Memory Usage: 71/976MB (7,27%)
#Disk Usage: 1592/6,0G (21%)
#CPU load: 0%
#Last boot: 2022-06-06 17:43
#LVM use: yes
#Connections TCP : 2 ESTABLISHED
#User log: 1
#Network: IP 192.168.0.160 (08:00:27:06:1c:19)
#Sudo : 25 cmd

Mensagem de broadcast de root@jvidon-n42 (somewhere) (Mon Jun  6 19:06:01 2022)

#Architecture: Linux jvidon-n42 5.10.0-14-amd64 #1 SMP Debian 5.10.113-1 (2022-04-29) x86_64
GNU/Linux
#CPU physical : 1
#vCPU : 1
#Memory Usage: 71/976MB (7,27%)
#Disk Usage: 1592/6,0G (21%)
#CPU load: 7%
#Last boot: 2022-06-06 17:43
#LVM use: yes
#Connections TCP : 2 ESTABLISHED
#User log: 1
#Network: IP 192.168.0.160 (08:00:27:06:1c:19)
#Sudo : 25 cmd
```

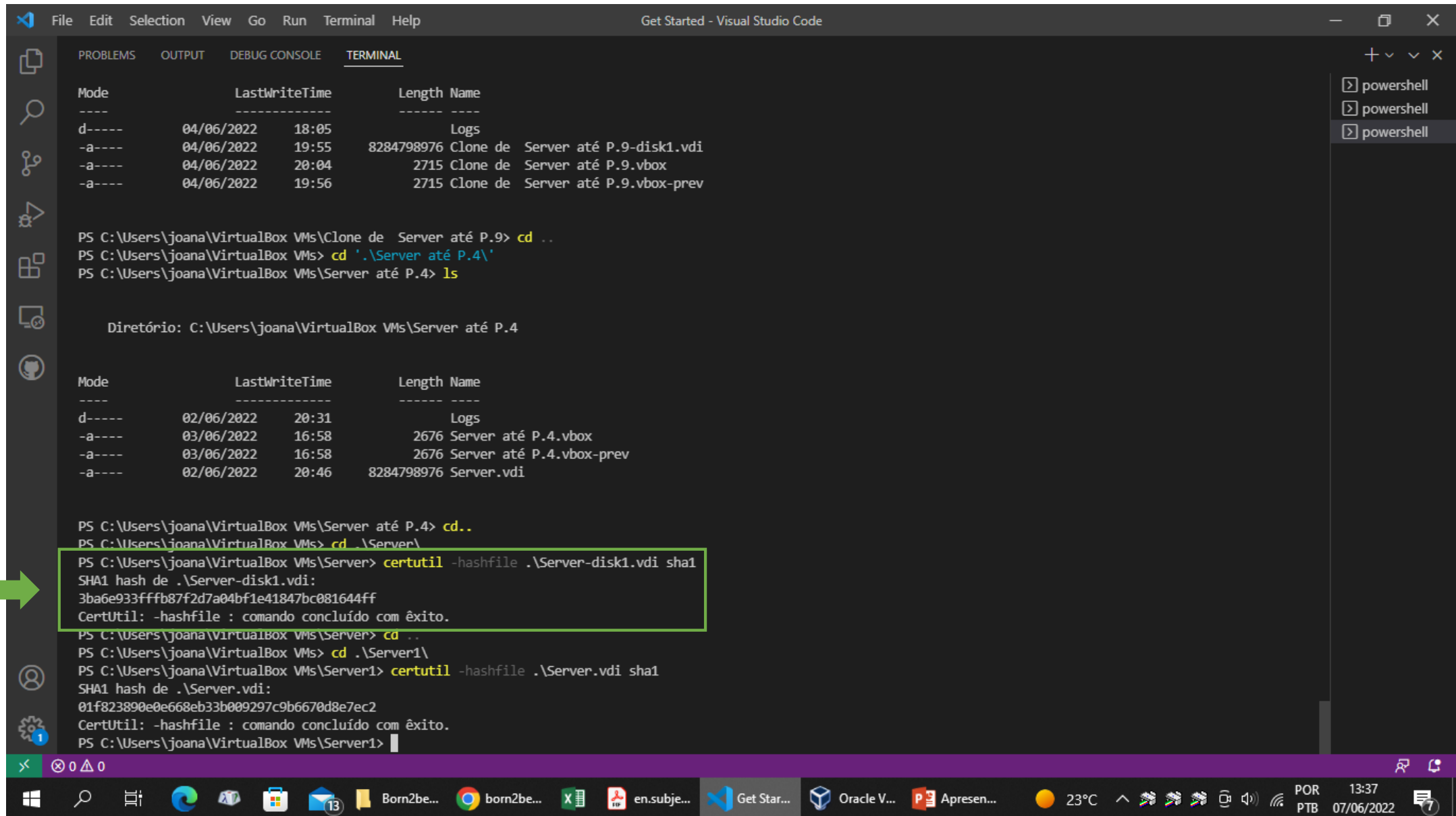
Teste feito com 2 minutos (`* /2 * * * *`)

```
* /2 * * * * bash /root/monitoring.sh
```

Para verificar: `crontab -l`

Para parar o cron, mas voltar a rodar após reboot:  
`/etc/init.d/cron stop`

# Assinatura



The screenshot shows the Visual Studio Code interface with a terminal window open. The terminal displays a series of commands and their outputs, including directory navigation and the execution of the `certutil` command to calculate SHA1 hashes of VDI files. A green arrow points to the `certutil` command line.

```
File Edit Selection View Go Run Terminal Help Get Started - Visual Studio Code
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL

Mode	LastWriteTime	Length	Name
d----	04/06/2022 18:05		Logs
-a----	04/06/2022 19:55	8284798976	Clone de Server até P.9-disk1.vdi
-a----	04/06/2022 20:04	2715	Clone de Server até P.9.vbox
-a----	04/06/2022 19:56	2715	Clone de Server até P.9.vbox-prev

```
PS C:\Users\joana\VirtualBox VMs\Clone de Server até P.9> cd ..
PS C:\Users\joana\VirtualBox VMs> cd '.\Server até P.4\'
PS C:\Users\joana\VirtualBox VMs\Server até P.4> ls
```

Diretório: C:\Users\joana\VirtualBox VMs\Server até P.4

Mode	LastWriteTime	Length	Name
d----	02/06/2022 20:31		Logs
-a----	03/06/2022 16:58	2676	Server até P.4.vbox
-a----	03/06/2022 16:58	2676	Server até P.4.vbox-prev
-a----	02/06/2022 20:46	8284798976	Server.vdi

```
PS C:\Users\joana\VirtualBox VMs\Server até P.4> cd..
PS C:\Users\joana\VirtualBox VMs> cd .\Server\
PS C:\Users\joana\VirtualBox VMs\Server> certutil -hashfile .\Server-disk1.vdi sha1
SHA1 hash de .\Server-disk1.vdi:
3ba6e933ffffb87f2d7a04bf1e41847bc081644ff
CertUtil: -hashfile : comando concluído com êxito.
PS C:\Users\joana\VirtualBox VMs\Server> cd ..
PS C:\Users\joana\VirtualBox VMs> cd .\Server\
PS C:\Users\joana\VirtualBox VMs\Server1> certutil -hashfile .\Server.vdi sha1
SHA1 hash de .\Server.vdi:
01f823890e0e668eb33b009297c9b6670d8e7ec2
CertUtil: -hashfile : comando concluído com êxito.
PS C:\Users\joana\VirtualBox VMs\Server1>
```

Taskbar: Born2be..., born2be..., en.subje..., Get Star..., Oracle V..., Apresen..., 23°C, 13:37, 07/06/2022

## **Alguns dos links usados:**

**Virtual box, o que é e como usar:**

<https://blog.b2bstack.com.br/virtualbox/>

**Apt e Aptude:**

<https://www.fosslinux.com/43884/apt-vs-aptitude.htm#:~:text=The%20first%20difference%20you%20will,by%20both%20of%20the%20tools.>

**SELinux:**

<https://www.redhat.com/pt-br/topics/linux/what-is-selinux>

**App Armor:**

<https://debian-handbook.info/browse/pt-BR/stable/sect.apparmor.html>

**Sudo:**

<https://mateusmuller.me/2019/11/06/sudo-guia-completo-do-comando-sudo-no-linux/>

<https://www.todoespacoonline.com/w/2015/10/su-sudo-e-sudoers-no-linux/>