



CURSO DE TECNOLOGIA EM DEFESA CIBERNÉTICA

ATIVIDADE DO CAP 9 – Mergulhando no bash

Kraków – Polônia

Maio/2021

Ian Alberto Ribeiro Christani

ATIVIDADE DO CAP 9 - Mergulhando no bash

Kraków – Polônia

Maio/2021

SUMÁRIO

1. INTRODUÇÃO.....4

2. DESENVOLVIMENTO.....5

3. CONCLUSÃO.....6

REFERÊNCIAS.....7

1 INTRODUÇÃO

A proposta dessa atividade é ter uma experiência com programação e automação no bash usando os conhecimentos acumulados no curso até então. Para isso, iremos programar uma rotina diária de backup de alguns arquivos estratégicos do nosso cliente.

2 DESENVOLVIMENTO

Os comandos inseridos na VM estão em negrito.

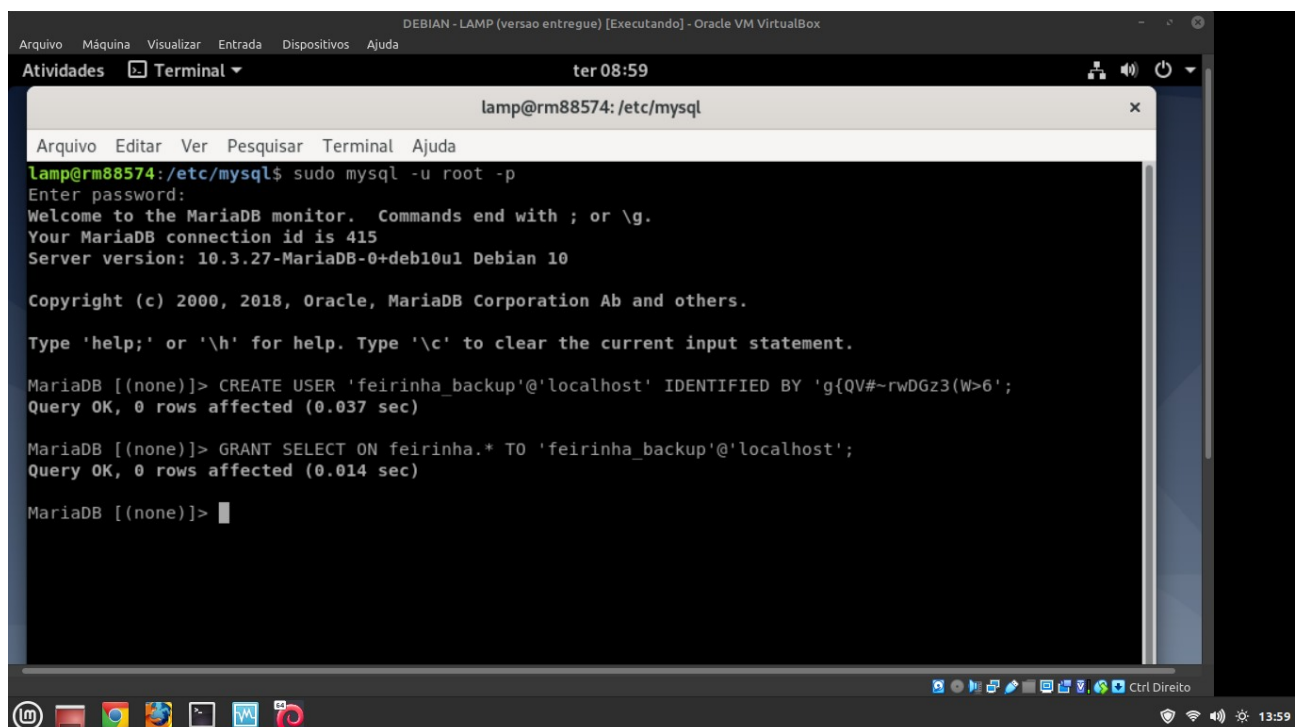
Vamos criar o usuário de consulta no MariaDB:

```
sudo mysql -u root -p
```

senha do admin do banco dbadmin (não o feirinha): +XT51Kh^QhT3hd1~

```
CREATE USER 'feirinha_backup'@'localhost' IDENTIFIED BY 'g{QV#~rwDGz3(W>6';
```

```
GRANT SELECT ON feirinha.* TO 'feirinha_backup'@'localhost';
```



The screenshot shows a terminal window titled "DEBIAN - LAMP (versao entregue) [Executando] - Oracle VM VirtualBox". The terminal is running a MySQL command prompt. The user 'lamp@rm88574' is in the directory '/etc/mysql'. The terminal shows the following commands and output:

```
lamp@rm88574:/etc/mysql$ sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 415
Server version: 10.3.27-MariaDB-0+deb10u1 Debian 10

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

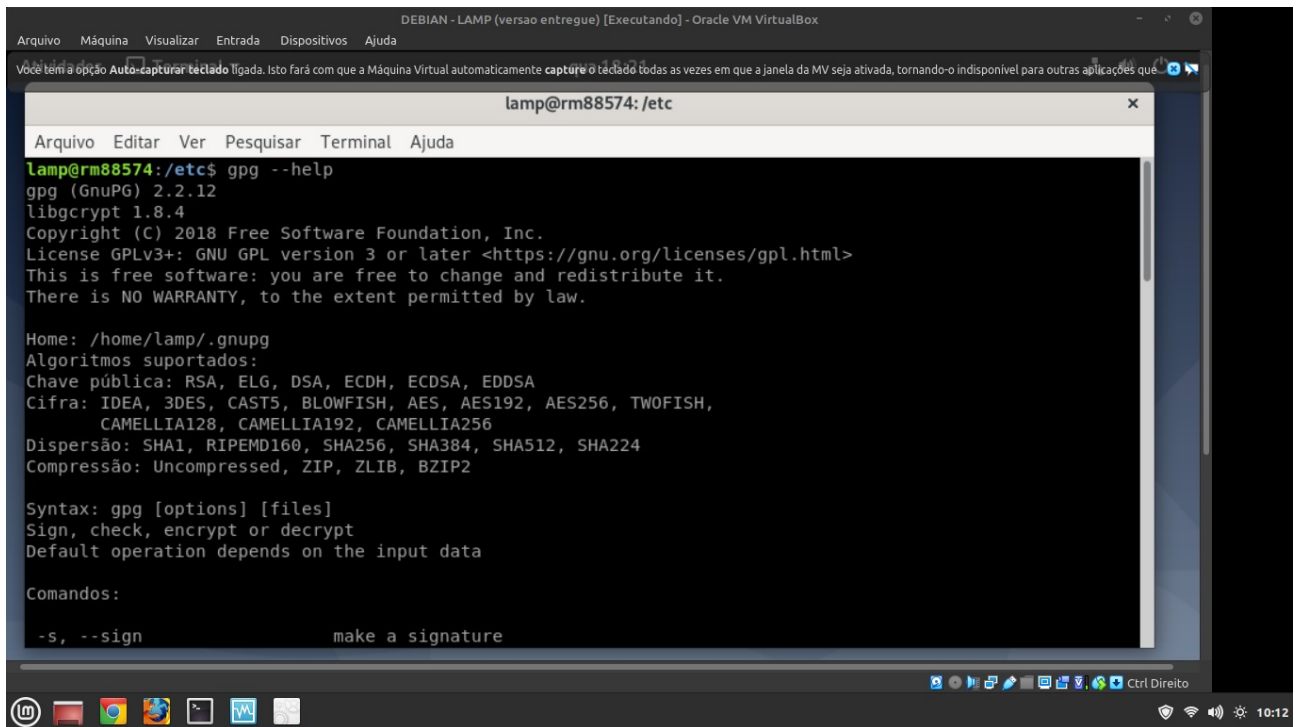
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> CREATE USER 'feirinha_backup'@'localhost' IDENTIFIED BY 'g{QV#~rwDGz3(W>6';
Query OK, 0 rows affected (0.037 sec)

MariaDB [(none)]> GRANT SELECT ON feirinha.* TO 'feirinha_backup'@'localhost';
Query OK, 0 rows affected (0.014 sec)

MariaDB [(none)]>
```

Para encriptarmos, vamos usar o programa GnuPG, que já encontra-se instalado:



```
DEBIAN - LAMP (versao entregue) [Executando] - Oracle VM VirtualBox
Arquivo Máquina Visualizar Entrada Dispositivos Ajuda
Você tem a opção Auto-capturar teclado ligada. Isto fará com que a Máquina Virtual automaticamente capture o teclado todas as vezes em que a janela da MV seja ativada, tornando-o indisponível para outras aplicações que...

lamp@rm88574: /etc
Arquivo Editar Ver Pesquisar Terminal Ajuda
lamp@rm88574:/etc$ gpg --help
gpg (GnuPG) 2.2.12
libgcrypt 1.8.4
Copyright (C) 2018 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <https://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

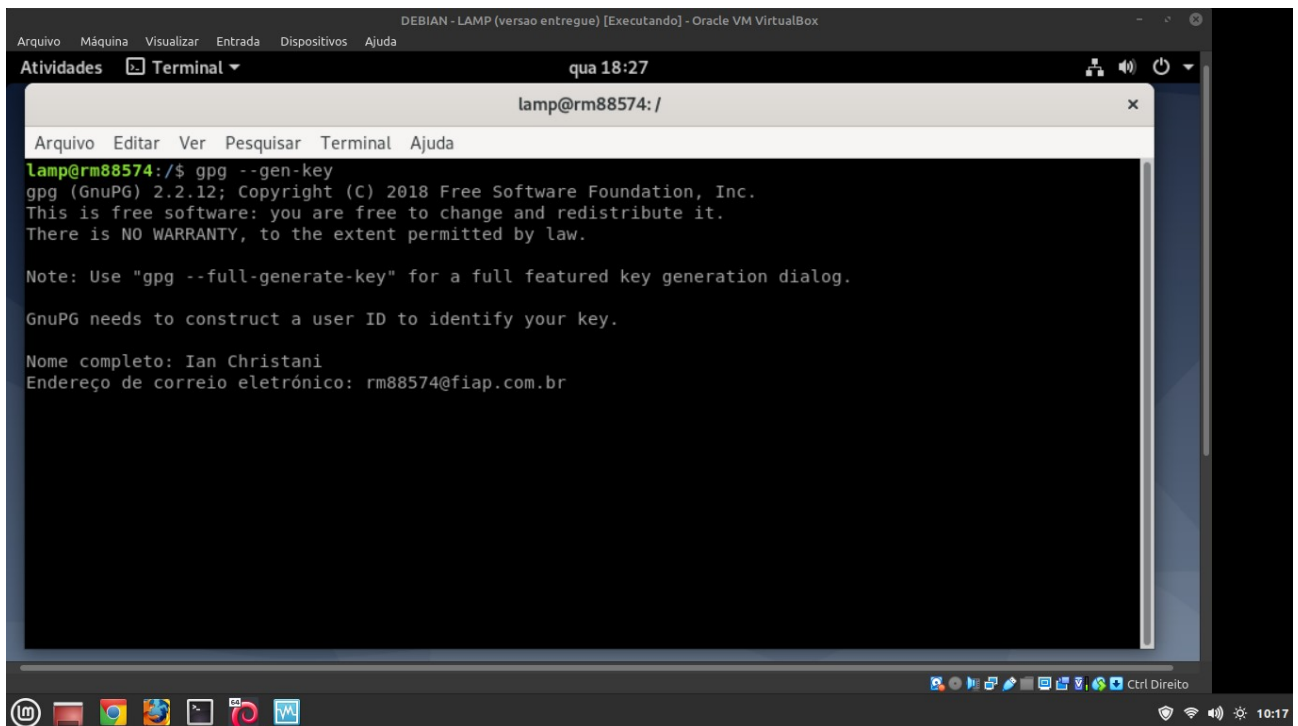
Home: /home/lamp/.gnupg
Algoritmos suportados:
Chave pública: RSA, ELG, DSA, ECDH, ECDSA, EDDSA
Cifra: IDEA, 3DES, CAST5, BLOWFISH, AES, AES192, AES256, TWOFISH,
      CAMELLIA128, CAMELLIA192, CAMELLIA256
Dispersão: SHA1, RIPEMD160, SHA256, SHA384, SHA512, SHA224
Compressão: Uncompressed, ZIP, ZLIB, BZIP2

Syntax: gpg [options] [files]
Sign, check, encrypt or decrypt
Default operation depends on the input data

Comandos:
-s, --sign                make a signature
```

Com isso vamos criar uma chave pública, que estará vinculada a um usuário que criaremos, para gerarmos os arquivos criptografados:

gpg --gen-key



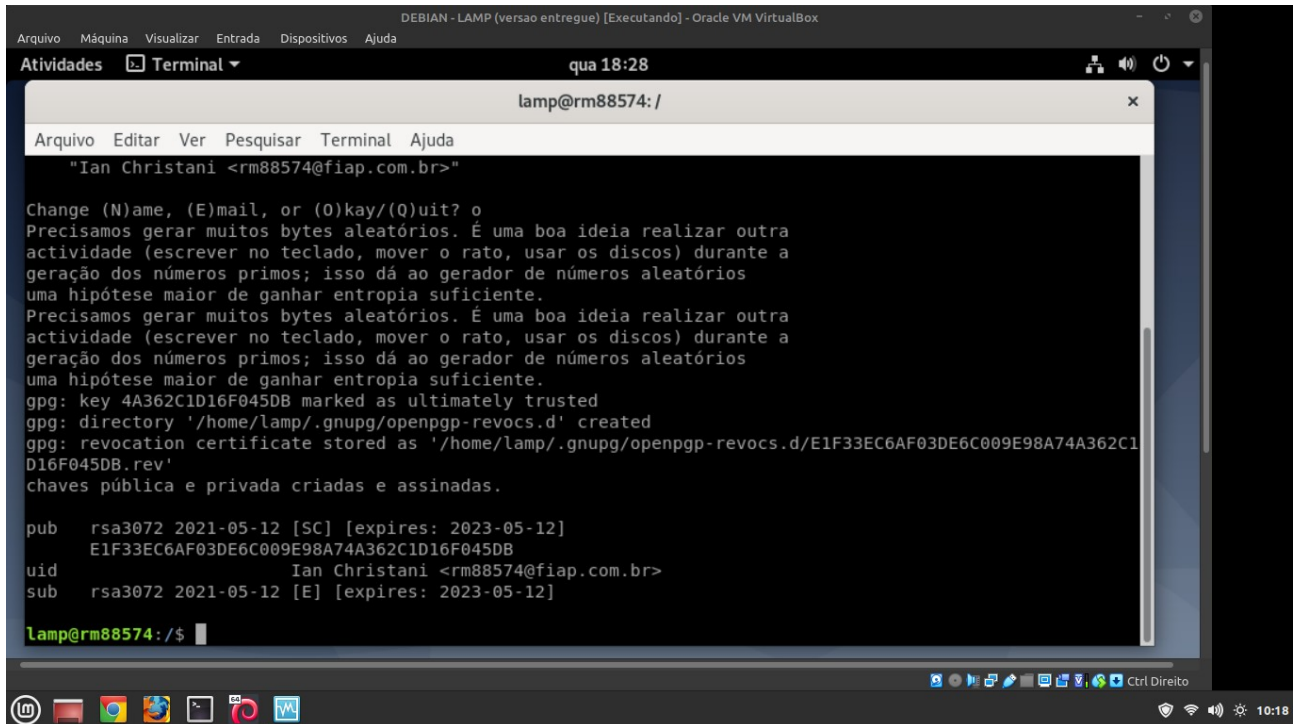
```
DEBIAN - LAMP (versao entregue) [Executando] - Oracle VM VirtualBox
Atividades Terminal
qua 18:27
lamp@rm88574: /
Arquivo Editar Ver Pesquisar Terminal Ajuda
lamp@rm88574:/$ gpg --gen-key
gpg (GnuPG) 2.2.12; Copyright (C) 2018 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Note: Use "gpg --full-generate-key" for a full featured key generation dialog.

GnuPG needs to construct a user ID to identify your key.

Nome completo: Ian Christani
Endereço de correio eletrônico: rm88574@fiap.com.br
```

Gerada a chave com o usuário:

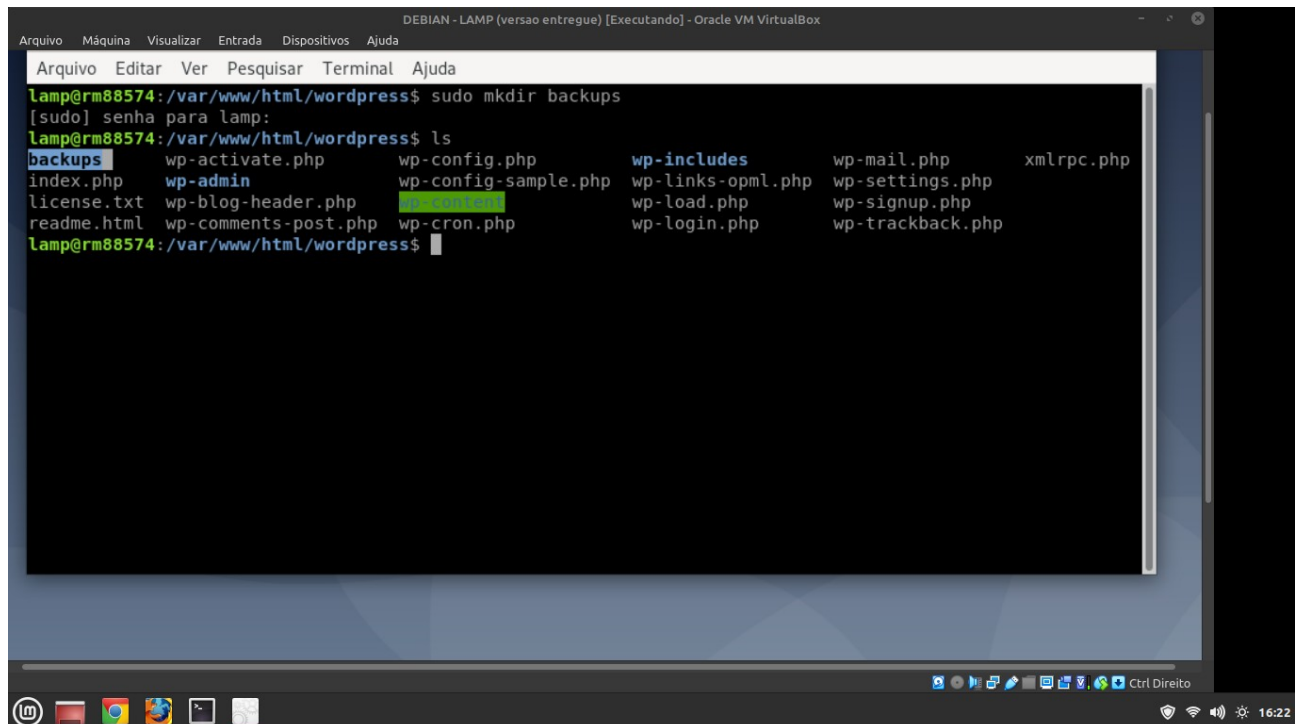


The screenshot shows a terminal window titled "DEBIAN - LAMP (versao entregue) [Executando] - Oracle VM VirtualBox". The terminal prompt is "lamp@rm88574: /". The user has entered the name "Ian Christani <rm88574@fiap.com.br>". The terminal output shows the GPG key generation process, including instructions to generate random bytes, the creation of a directory for revocations, and the storage of the revocation certificate. The final output shows the public and private keys created and signed.

```
lamp@rm88574: /  
Arquivo Editar Ver Pesquisar Terminal Ajuda  
"Ian Christani <rm88574@fiap.com.br>"  
  
Change (N)ame, (E)mail, or (O)kay/(Q)uit? o  
Precisamos gerar muitos bytes aleatórios. É uma boa ideia realizar outra  
actividade (escrever no teclado, mover o rato, usar os discos) durante a  
geração dos números primos; isso dá ao gerador de números aleatórios  
uma hipótese maior de ganhar entropia suficiente.  
Precisamos gerar muitos bytes aleatórios. É uma boa ideia realizar outra  
actividade (escrever no teclado, mover o rato, usar os discos) durante a  
geração dos números primos; isso dá ao gerador de números aleatórios  
uma hipótese maior de ganhar entropia suficiente.  
gpg: key 4A362C1D16F045DB marked as ultimately trusted  
gpg: directory '/home/lamp/.gnupg/openpgp-revocs.d' created  
gpg: revocation certificate stored as '/home/lamp/.gnupg/openpgp-revocs.d/E1F33EC6AF03DE6C009E98A74A362C1D16F045DB.rev'  
chaves pública e privada criadas e assinadas.  
  
pub   rsa3072 2021-05-12 [SC] [expires: 2023-05-12]  
      E1F33EC6AF03DE6C009E98A74A362C1D16F045DB  
uid           Ian Christani <rm88574@fiap.com.br>  
sub   rsa3072 2021-05-12 [E] [expires: 2023-05-12]  
  
lamp@rm88574:/$
```

Vamos criar o diretório onde ficarão os arquivos de backup e o script, esta pasta estará dentro da pasta do wordpress. De certo não é o melhor lugar para alocar tal tipo de diretório, mas a título de experimento é válido:

sudo mkdir backups



```
DEBIAN - LAMP (versao entregue) [Executando] - Oracle VM VirtualBox
Arquivo  Máquina  Visualizar  Entrada  Dispositivos  Ajuda
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda
lamp@rm88574:/var/www/html/wordpress$ sudo mkdir backups
[sudo] senha para lamp:
lamp@rm88574:/var/www/html/wordpress$ ls
backups      wp-activate.php      wp-config.php      wp-includes      wp-mail.php      xmlrpc.php
index.php    wp-admin              wp-config-sample.php wp-links-opml.php wp-settings.php
license.txt  wp-blog-header.php    wp-content          wp-load.php      wp-signup.php
readme.html  wp-comments-post.php  wp-cron.php        wp-login.php     wp-trackback.php
lamp@rm88574:/var/www/html/wordpress$
```

Vamos agora criar o arquivo de script da rotina:

sudo vi script

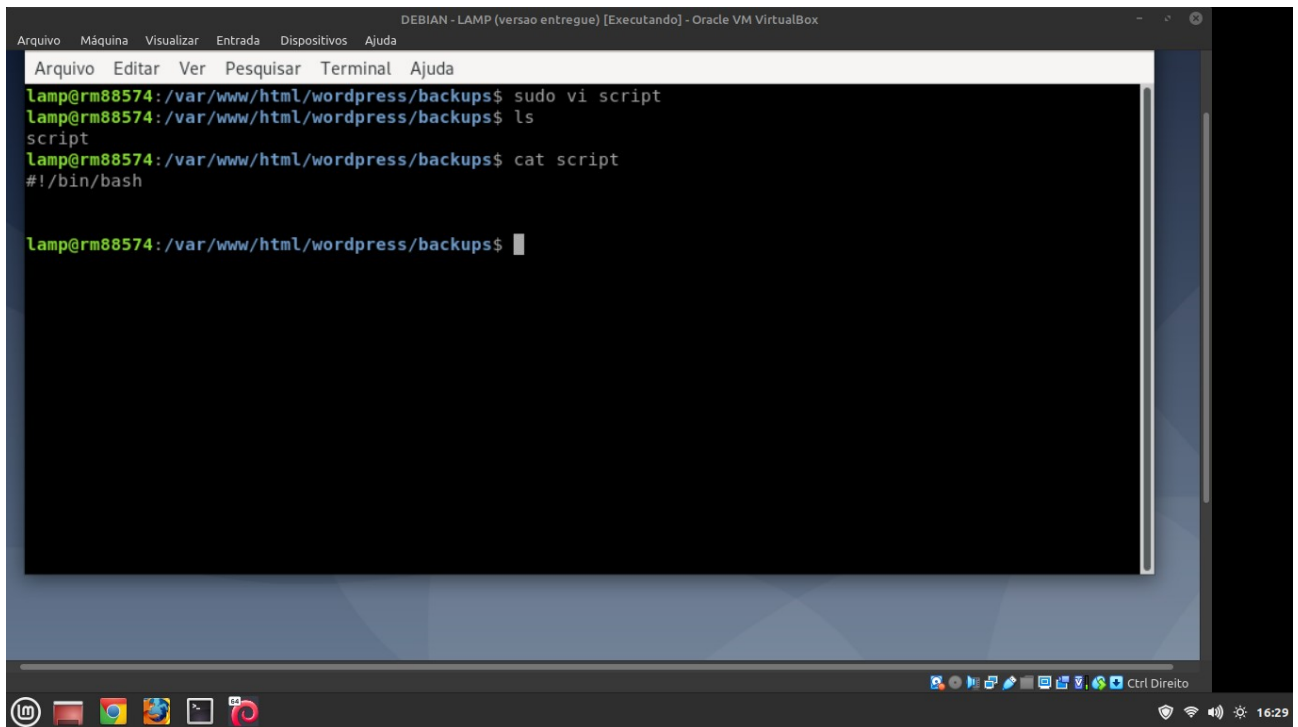
dentro do arquivo:

#!/bin/bash

agora no bash:

ls

cat script



```

DEBIAN - LAMP (versao entregue) [Executando] - Oracle VM VirtualBox
Arquivo  Máquina  Visualizar  Entrada  Dispositivos  Ajuda
lamp@rm88574:/var/www/html/wordpress/backups$ sudo vi script
lamp@rm88574:/var/www/html/wordpress/backups$ ls
script
lamp@rm88574:/var/www/html/wordpress/backups$ cat script
#!/bin/bash

lamp@rm88574:/var/www/html/wordpress/backups$

```

Para fazermos um backup seguro temos que encriptar os arquivos e para isso usaremos o PGP, que já encontra-se instalado na máquina. Vamos fazer primeiramente a compactação dos arquivos e posteriormente encriptá-los.

Dentro do arquivo script recém criado vamos editá-lo da mesma forma e adicionar:

#trabalhando no diretório de backup

cd /var/www/html/wordpress/backups/

#criando a variavel de data

data=\$(date +%y-%m-%d)

#criando o diretório de armazenamento de cada backup diário

mkdir /var/www/html/wordpress/backups/bk\$data

cd /var/www/html/wordpress/backups/bk\$data

#criando o dump do banco de dados

```
mysqldump feirinha -u feirinha_backup \  
--password='g{QV#~rwDGz3(W>6'>feirinha_mysql_${data}.dump
```

```
#compactando o banco de dados
```

```
bzip2 -z -f feirinha_mysql_${data}.dump
```

```
#encriptando o arquivo
```

```
gpg --yes -e -r rm88574@fiap.com.br feirinha_mysql_${data}.dump.bz2
```

```
#ajustando o nome para atender ao enunciado
```

```
mv feirinha_mysql_${data}.dump.bz2.gpg feirinha_mysql_${data}.dump.bz2
```

```
#compactando os arquivos do site e wordpress
```

```
tar -cjf feirinha_${data}.tar.bz2 -C / var/www/html/wordpress/
```

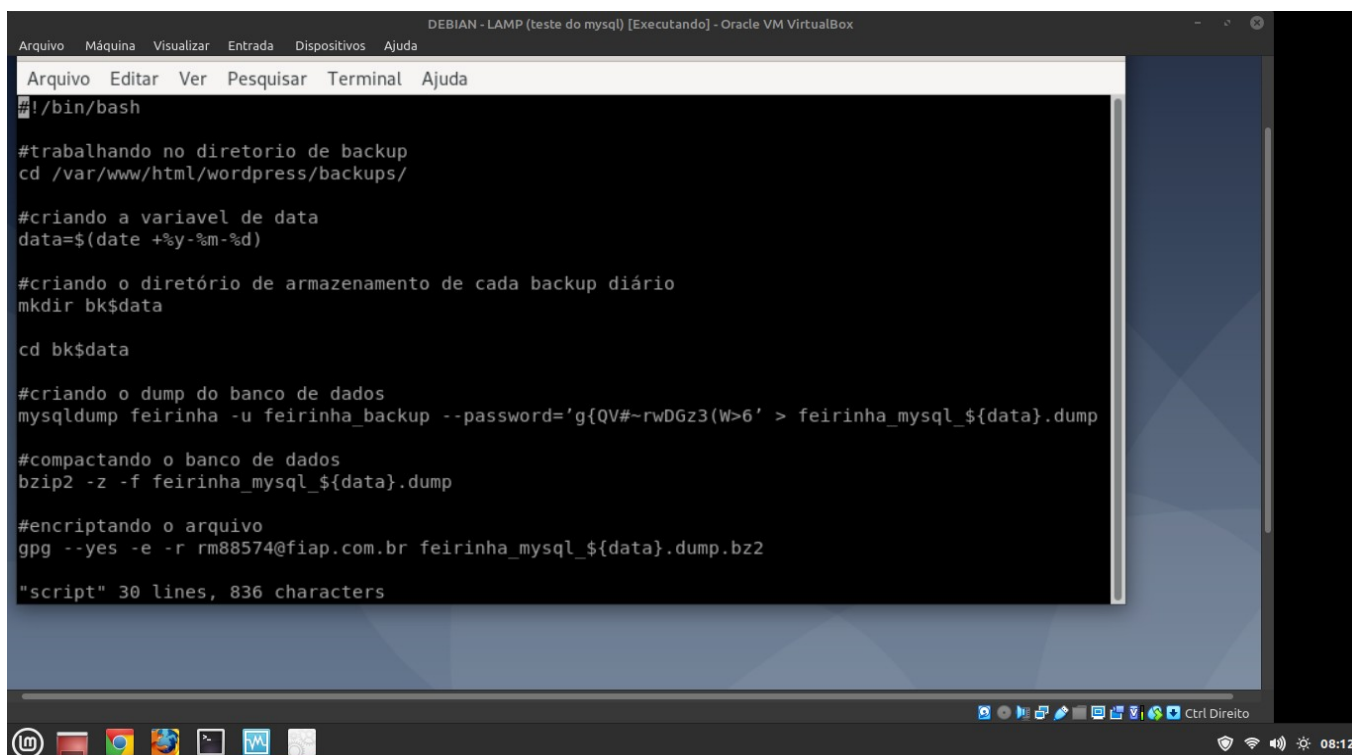
```
#encriptando o arquivo
```

```
gpg --yes -e -r rm88574@fiap.com.br feirinha_${data}.tar.bz2
```

```
#ajustando o nome para atender ao enunciado
```

```
rm -r feirinha_${data}.tar.bz2
```

```
mv feirinha_${data}.tar.bz2.gpg feirinha_${data}.tar.bz2
```



```
DEBIAN - LAMP (teste do mysql) [Executando] - Oracle VM VirtualBox
Arquivo  Máquina  Visualizar  Entrada  Dispositivos  Ajuda

Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda

#!/bin/bash

#trabalhando no diretorio de backup
cd /var/www/html/wordpress/backups/

#criando a variavel de data
data=$(date +%y-%m-%d)

#criando o diretório de armazenamento de cada backup diário
mkdir bk$data

cd bk$data

#criando o dump do banco de dados
mysqldump feirinha -u feirinha_backup --password='g{QV#~rwDGz3(W>6' > feirinha_mysql_${data}.dump

#compactando o banco de dados
bzip2 -z -f feirinha_mysql_${data}.dump

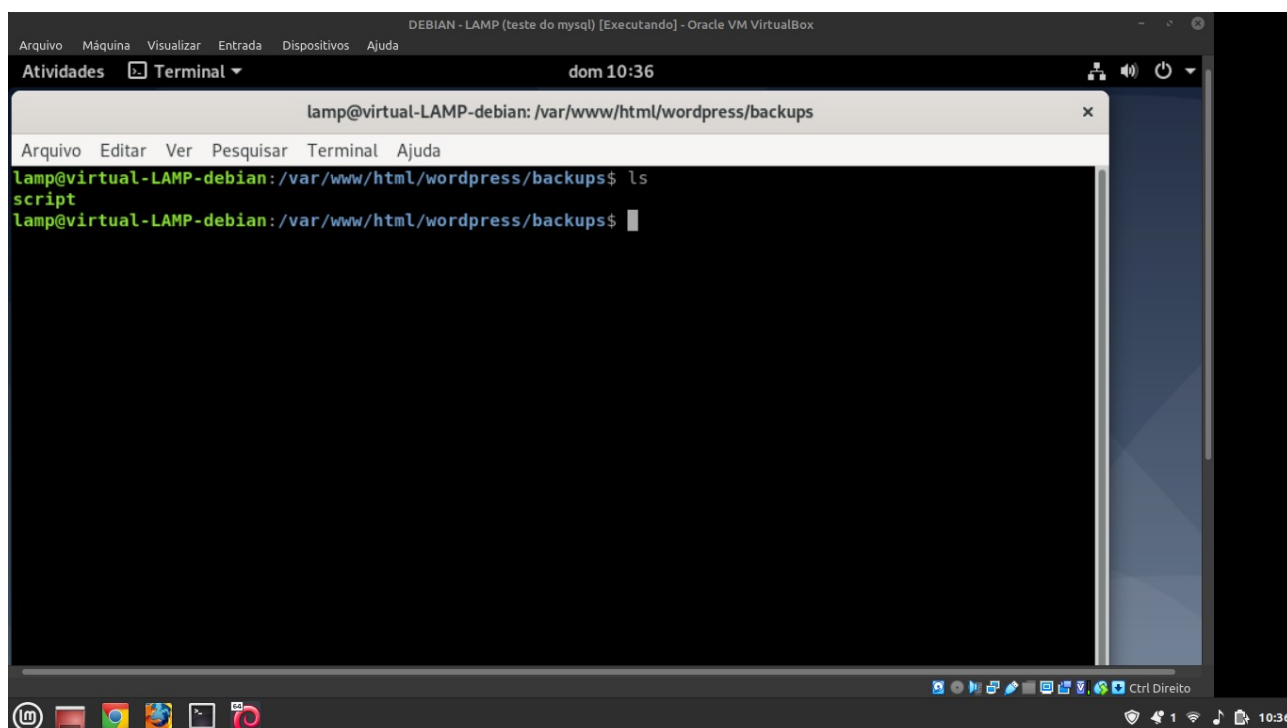
#encriptando o arquivo
gpg --yes -e -r rm88574@fiap.com.br feirinha_mysql_${data}.dump.bz2

"script" 30 lines, 836 characters
```

Vamos alterar a permissão do arquivo, para possibilitar sua execução:

sudo chmod u+x script

Feito isto, agora vamos fazer um teste com o CRONTAB antes da programação final:



```
DEBIAN - LAMP (teste do mysql) [Executando] - Oracle VM VirtualBox
Atividades  Terminal  dom 10:36

lamp@virtual-LAMP-debian: /var/www/html/wordpress/backups

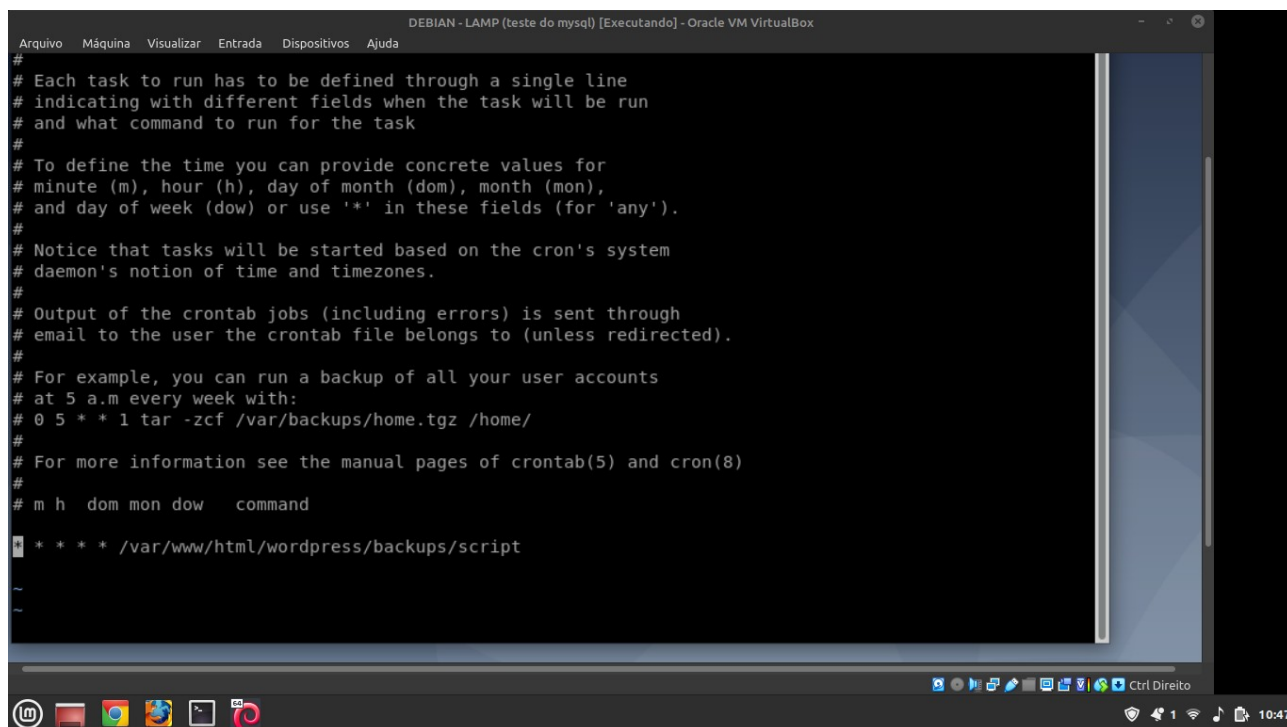
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda

lamp@virtual-LAMP-debian:/var/www/html/wordpress/backups$ ls
script
lamp@virtual-LAMP-debian:/var/www/html/wordpress/backups$
```

cd /etc/

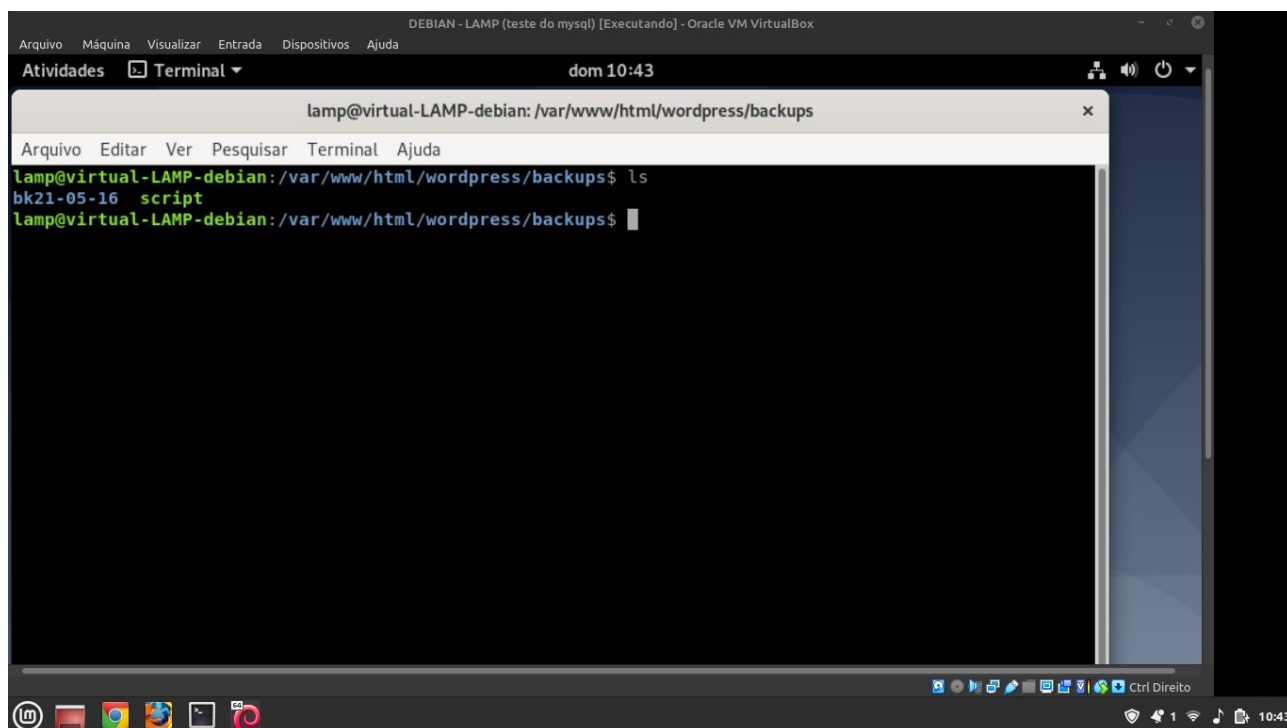
sudo crontab -e

*** * * * * /var/www/html/wordpress/backups/script**

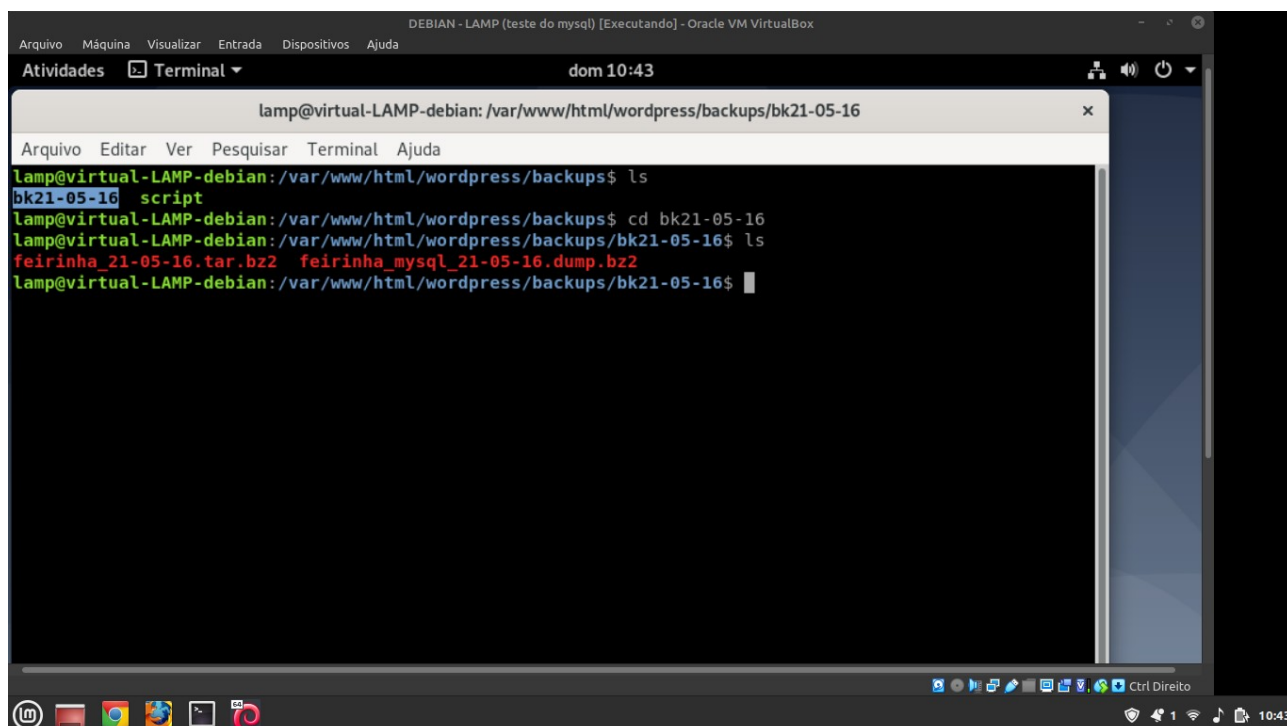


```
Arquivo  Máquina  Visualizar  Entrada  Dispositivos  Ajuda
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h dom mon dow   command
* * * * * /var/www/html/wordpress/backups/script
~
~
```

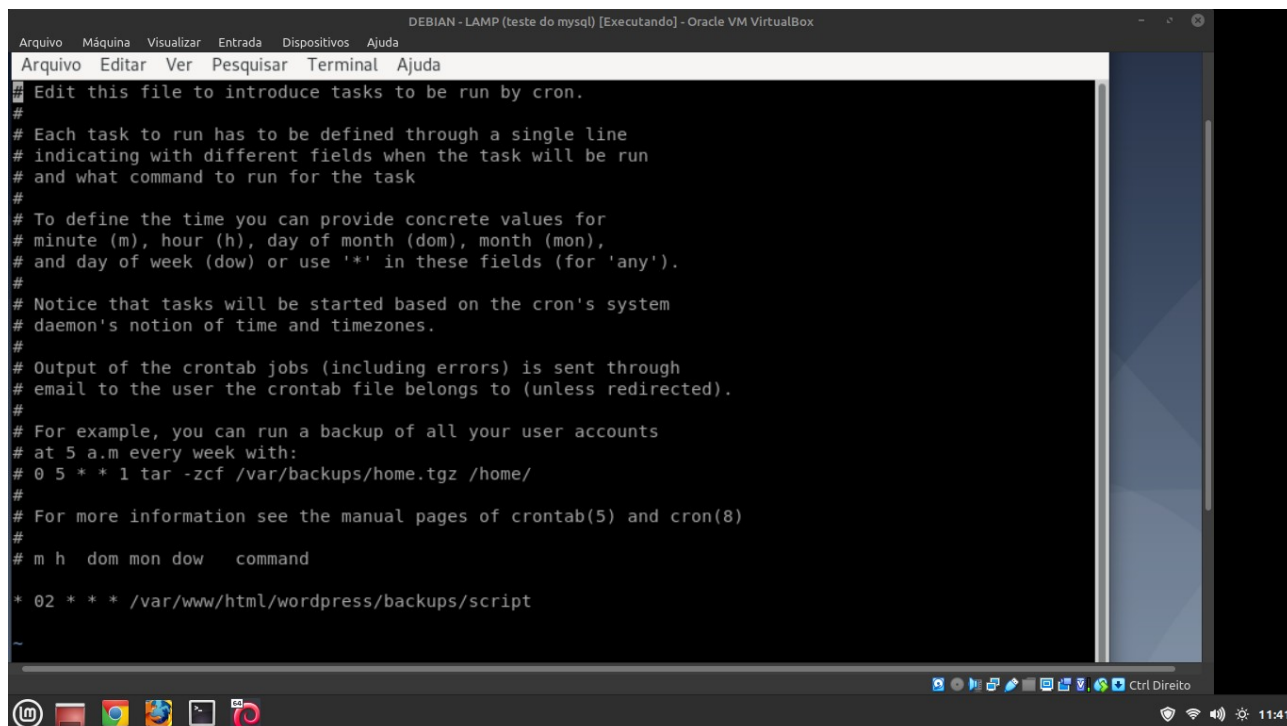
Vimos que deu certo:



Dentro da pasta contém:



Agora vamos ajustar para a frequência pedida no enunciado:



```
DEBIAN - LAMP (teste do mysql) [Executando] - Oracle VM VirtualBox
Arquivo  Máquina  Visualizar  Entrada  Dispositivos  Ajuda
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h dom mon dow   command
* 02 * * * /var/www/html/wordpress/backups/script
```

Agora todos os dias a 2 da manhã ele realizará o backup de acordo com o que programamos no script.

3 CONCLUSÃO

Com este trabalho pudemos ter a experiência de automatizar uma rotina no bash e ter contato com alguns aplicativos estratégicos como de criptografia, compactação, que são essenciais na rotina de um profissional de cibersegurança e agendamento de rotinas dentro do sistema operacional.

PS: Estou feliz pra caramba! Porque ao olhar o meu conhecimento quando comecei o curso eu não tinha a menor noção de como fazer isso! (emocionado)

Desculpe, tive que colocar aqui! :)

REFERÊNCIAS

Material de estudos do curso de Segurança Cibernética da FIAP – Fase 3 cap 10 ao cap 13;