

Compte rendu du projet

Administration Réseau :

Configuration d'un serveur WEB



- Réalisé par :
Ayoub EL HADDADI

- Configuration de Putty:

← → ↻ ⚠ Non sécurisé | jenkins.chebrek.com:8080/login?from=%2F



Bienvenue dans Jenkins !

Utilisateur

Mot de passe

☐ Garder ma session ouverte

S'identifier

✓ Build Telnet (17 nov. 2022 à 13:02:45)

InstanceID : i-073581ac8251ebae2
Web - Ayoub EL HADDADI
PublicIP : 13.37.212.37
PrivateIP : 172.31.35.39



Lancé par l'utilisateur

PuTTY Configuration

Category:

- Colours
- Connection
 - Data
 - Proxy
 - SSH
 - Kex
 - Host keys
 - Cipher
 - Auth
 - Credenti.
 - GSSAPI
 - TTY
 - X11
 - Tunnels
 - Bugs
 - More bugs
 - Serial
 - Telnet
 - Rlogin
 - SUPDUP

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address) Port

13.37.212.37 22

Connection type:

☒ SSH ☐ Serial ☐ Other: Telnet

Load, save or delete a stored session

Saved Sessions

Default Settings

Load Save Delete

Close window on exit:

☐ Always ☐ Never ☒ Only on clean exit

About Open Cancel

```
admin@ip-172-31-35-39: ~  
login as: admin  
Authenticating with public key "Telnet"  
Linux ip-172-31-35-39 5.10.0-19-cloud-amd64 #1 SMP Debian 5.10.149-2 (2022-10-21) 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 Nov 25 21:40:36 2022 from 27.122.12.254  
admin@ip-172-31-35-39:~$
```

I. Création des comptes utilisateurs :

Tout d'abord, nous devons faire la mise à jour pour des raisons de performances et de sécurité. pour cela nous allons utiliser deux commandes principales :

```
admin@ip-172-31-35-39:~$ sudo apt-get update  
Hit:1 http://cdn-aws.deb.debian.org/debian bullseye InRelease  
Get:2 http://cdn-aws.deb.debian.org/debian bullseye-updates InRelease [44.1 kB]  
Get:3 http://security.debian.org/debian-security bullseye-security InRelease [48  
.4 kB]  
Get:4 http://cdn-aws.deb.debian.org/debian bullseye-backports InRelease [49.0 kB  
]  
Get:5 http://cdn-aws.deb.debian.org/debian bullseye-backports/main Sources.diff/  
Index [63.3 kB]  
Get:6 http://cdn-aws.deb.debian.org/debian bullseye-backports/main amd64 Package  
s.diff/Index [63.3 kB]
```

sudo apt-get update télécharge les paquets des dépôts et les met à jour pour obtenir des informations sur les versions les plus récentes des paquets et leurs dépendances.

```

admin@ip-172-31-35-39:~$ sudo apt-get upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages will be upgraded:
  grub-efi-amd64-signed libc-bin libc-l10n libc6 libgssapi-krb5-2 libk5crypto3
  libkrb5-3 libkrb5support0 locales tzdata
10 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 8888 kB/10.1 MB of archives.
After this operation, 10.2 kB disk space will be freed.
Do you want to continue? [Y/n] Y
Get:1 http://cdn-aws.deb.debian.org/debian bullseye-updates/main amd64 libc6 amd
64 2.31-13+deb11u5 [2825 kB]

```

sudo apt-get upgrade installe les nouvelles versions des paquets existants sur la machine.

Maintenant, nous passons à la création des comptes utilisateurs, pour cela nous utiliserons la commande : sudo adduser userName. Cette commande doit être invoquée par un compte d'administration.

```

admin@ip-172-31-35-39:~$ sudo adduser ayoub
Adding user `ayoub' ...
Adding new group `ayoub' (1001) ...
Adding new user `ayoub' (1001) with group `ayoub' ...
The home directory `/home/ayoub' already exists. Not copying from `/etc/skel'.
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for ayoub
Enter the new value, or press ENTER for the default
  Full Name []: Ayoub EL HADDADI
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Is the information correct? [Y/n] Y

```

De même, nous allons créer les autres utilisateurs : **alexis**, **mohamed**, **ikram**, **adnen** et **oumayma**.

- Le mot de passe du compte alexis est : **alexis01**

II. Affectation des droits administrateurs :

Nous avons deux types de comptes: l'un a les droits de créer et modifier les fichiers, l'autre n'a pas le droit de modifier sur les fichiers surtout les fichiers de configuration. Pour séparer ces deux types de comptes, nous allons les affecter sur deux groupes. Un groupe contient les

administrateurs et un groupe contient les utilisateurs.

Alors, c'est le temps de créer un groupe. La commande `sudo addgroup groupName`, invoquée par un compte d'administration, démarre le script de création de groupe d'utilisateurs

Maintenant, nous voulons ajouter les nouveaux utilisateurs au groupe membres. Pour cela nous allons profiter de la commande `usermod`.

Cette commande est assez simple à utiliser: `sudo usermod -aG groupName userName`

```
admin@ip-172-31-35-39:~$ sudo usermod -aG sudo alexis
admin@ip-172-31-35-39:~$ sudo usermod -aG sudo ayoub
admin@ip-172-31-35-39:~$ sudo usermod -aG membres ikram
admin@ip-172-31-35-39:~$ sudo usermod -aG membres adnen
admin@ip-172-31-35-39:~$ sudo usermod -aG membres mohamed
admin@ip-172-31-35-39:~$ sudo usermod -aG membres oumayma
```

Le groupe `sudo` existe déjà dans la machine et contient les comptes d'administration.

Pour vérifier que l'affectation a été bien réalisé avec succès, on affiche les utilisateurs des groupes `membres` et `sudo` à l'aide de la commande : `grep groupName /etc/group`.

```
admin@ip-172-31-35-39:~$ grep sudo /etc/group
sudo:x:27:admin,alexis,ayoub
admin@ip-172-31-35-39:~$ grep membres /etc/group
membres:x:1007:ikram,adnen,mohamed,oumayma
```

III. Configuration du SSH:

Pour permettre aux nouveaux utilisateurs et aux administrateurs d'accéder à la machine via SSH en utilisant leur mot de passe que nous avons déjà attribué lors de la phase de création des comptes, nous allons modifier le fichier `/etc/ssh/sshd_config` en ajoutant les deux lignes suivantes :

- `sudo nano /etc/ssh/sshd_config` va nous permet d'ouvrir le fichier `sshd_config` et d'activer l'option du "PasswordAuthentication" en changeant "no" par "yes" :


```
#IgnoreRhosts yes

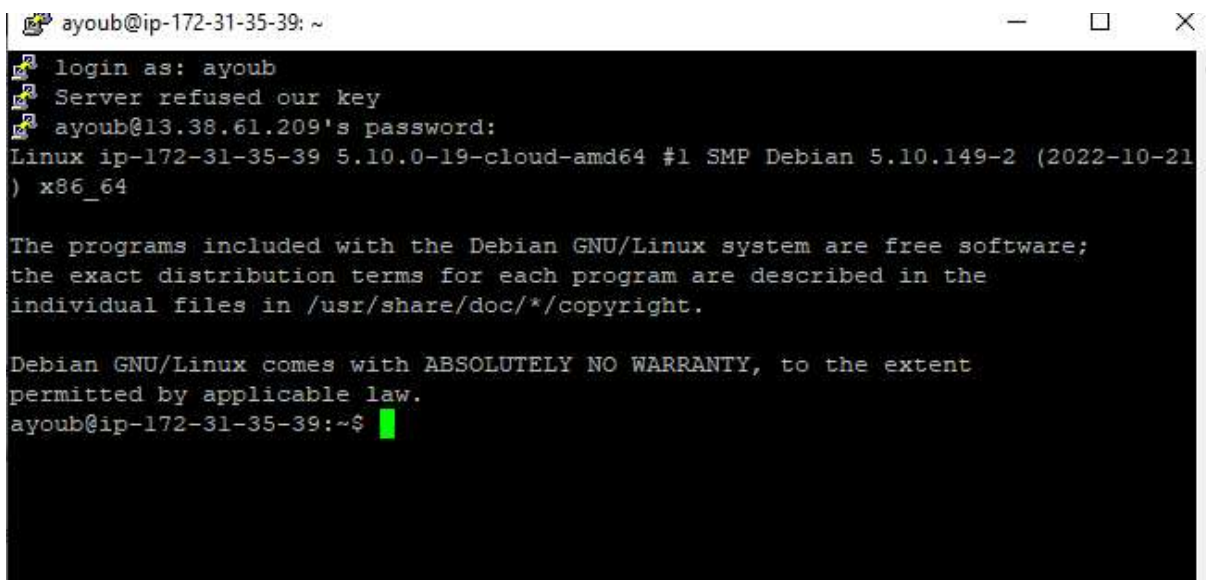
# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication yes
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
```

- `sudo echo "AllowGroup sudo membres">> /etc/ssh/sshd` va ajouter la ligne à la fin du fichier en permettant l'accès aux administrateurs et aux utilisateurs des groupes mentionnés :

```
root@ip-172-31-35-39:/home/admin# sudo echo "AllowGroup sudo membres">> /etc/ssh
/sshd
root@ip-172-31-35-39:/home/admin# ls /etc/ssh/
moduli          ssh_host_ecdsa_key      ssh_host_rsa_key.pub
ssh_config      ssh_host_ecdsa_key.pub  sshd
ssh_config.d    ssh_host_ed25519_key    sshd_config
ssh_host_dsa_key ssh_host_ed25519_key.pub sshd_config.d
ssh_host_dsa_key.pub ssh_host_rsa_key        sshd_config.ucf-dist
```

- Demande du mot de passe à la connection SSH



```
ayoub@ip-172-31-35-39: ~
login as: ayoub
Server refused our key
ayoub@13.38.61.209's password:
Linux ip-172-31-35-39 5.10.0-19-cloud-amd64 #1 SMP Debian 5.10.149-2 (2022-10-21)
) 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.
ayoub@ip-172-31-35-39:~$
```

IV. Installation et configuration du fail2ban :

Pour installer fail2ban, nous utiliserons la commande `sudo apt-get install fail2ban`.

```
ayoub@ip-172-31-35-39: ~
Get:4 http://cdn-aws.deb.debian.org/debian bullseye/main amd64 whois amd64 5.5.1
0 [81.1 kB]
Fetched 596 kB in 0s (5018 kB/s)
Selecting previously unselected package fail2ban.
(Reading database ... 30796 files and directories currently installed.)
Preparing to unpack .../fail2ban_0.11.2-2_all.deb ...
Unpacking fail2ban (0.11.2-2) ...
Selecting previously unselected package python3-pyinotify.
Preparing to unpack .../python3-pyinotify_0.9.6-1.3_all.deb ...
Unpacking python3-pyinotify (0.9.6-1.3) ...
Selecting previously unselected package python3-systemd.
Preparing to unpack .../python3-systemd_234-3+b4_amd64.deb ...
Unpacking python3-systemd (234-3+b4) ...
Selecting previously unselected package whois.
Preparing to unpack .../whois_5.5.10_amd64.deb ...
Unpacking whois (5.5.10) ...
Setting up whois (5.5.10) ...
Setting up fail2ban (0.11.2-2) ...
Created symlink /etc/systemd/system/multi-user.target.wants/fail2ban.service → /
lib/systemd/system/fail2ban.service.
Setting up python3-pyinotify (0.9.6-1.3) ...
Setting up python3-systemd (234-3+b4) ...
Processing triggers for man-db (2.9.4-2) ...
```

Pour vérifier l'état de fail2ban, nous utiliserons la commande `sudo systemctl status fail2ban`.

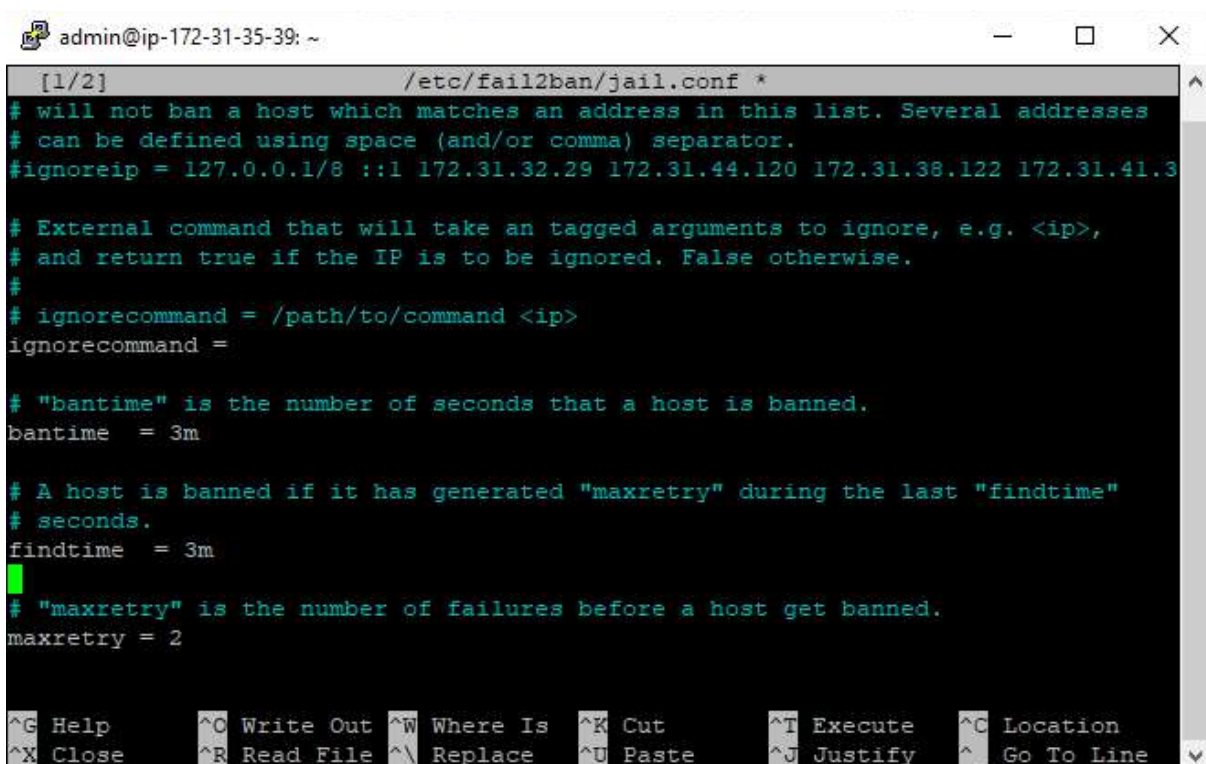
```
ayoub@ip-172-31-35-39:~$ sudo systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
   Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; vendor pres
   Active: active (running) since Fri 2022-11-25 21:47:56 UTC; 44s ago
     Docs: man:fail2ban(1)
    Process: 834 ExecStartPre=/bin/mkdir -p /run/fail2ban (code=exited, status=
   Main PID: 835 (fail2ban-server)
      Tasks: 5 (limit: 1123)
     Memory: 18.1M
        CPU: 245ms
    CGroup: /system.slice/fail2ban.service
            └─835 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

Nov 25 21:47:56 ip-172-31-35-39 systemd[1]: Starting Fail2Ban Service...
Nov 25 21:47:56 ip-172-31-35-39 systemd[1]: Started Fail2Ban Service.
Nov 25 21:47:57 ip-172-31-35-39 fail2ban-server[835]: Server ready
lines 1-15/15 (END)
```

La configuration Fail2ban se trouve dans le fichier [/etc/fail2ban/jail.conf](#) mais, il se peut que le fichier soit écrasé lors d'une mise à jour du package. On va donc créer une copie de ce fichier (avec l'extension .local) pour remplacer les paramètres du fichier .conf

Pour copier le fichier [jail.conf](#) dans un nouveau fichier [jail.local](#), on utilise la commande: `sudo cp /etc/fail2ban/jail.{conf,local}`, on peut ouvrir ensuite le fichier pour le modifier par la commande `sudo nano /etc/fail2ban/jail.{conf,local}`

```
ayoub@ip-172-31-35-39:~$ sudo cp /etc/fail2ban/jail.{conf,local}
ayoub@ip-172-31-35-39:~$ sudo nano /etc/fail2ban/jail.{conf,local}
```



```
[1/2] /etc/fail2ban/jail.conf *
# will not ban a host which matches an address in this list. Several addresses
# can be defined using space (and/or comma) separator.
#ignoreip = 127.0.0.1/8 ::1 172.31.32.29 172.31.44.120 172.31.38.122 172.31.41.3

# External command that will take an tagged arguments to ignore, e.g. <ip>,
# and return true if the IP is to be ignored. False otherwise.
#
# ignorecommand = /path/to/command <ip>
ignorecommand =

# "bantime" is the number of seconds that a host is banned.
bantime = 3m

# A host is banned if it has generated "maxretry" during the last "findtime"
# seconds.
findtime = 3m

# "maxretry" is the number of failures before a host get banned.
maxretry = 2

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Close     ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line
```

[ignoreip](#) définit la suite d'adresses IP qui ne se feront jamais bannir,

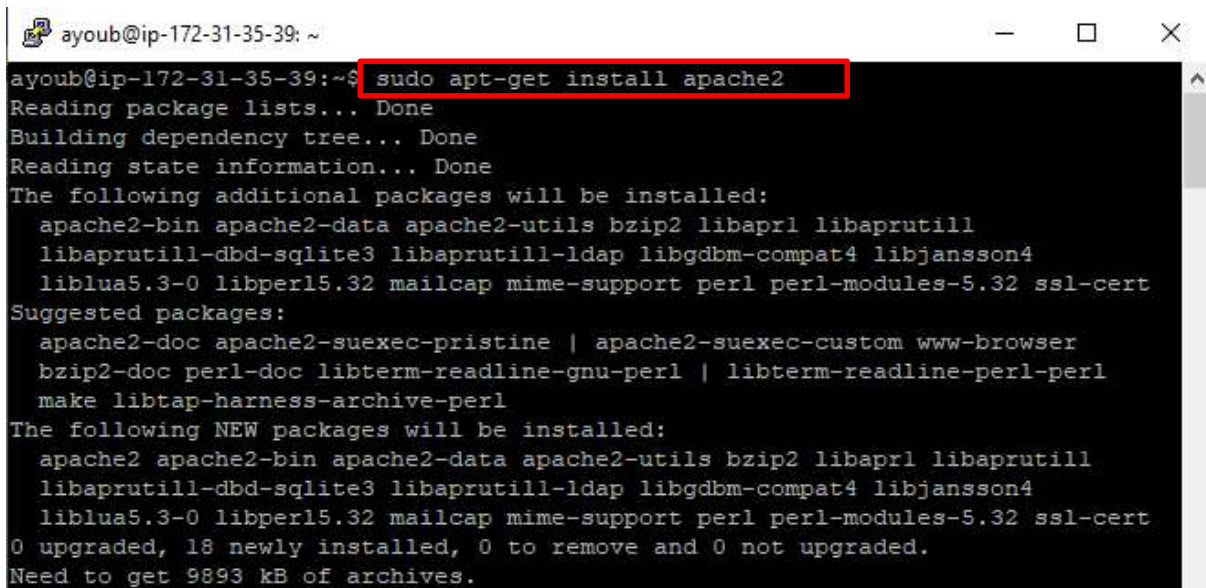
[bantime](#) définit le temps d'interdiction,

[findtime](#) définit la période pendant laquelle les essais vont incrémenter maxretry,

[maxretry](#) définit le maximum des tentatives avant qu'il soit interdit.

V. Configuration du serveur web :

Pour installer Apache, nous utiliserons la commande [sudo apt-get install apache2](#)

A terminal window with a black background and white text. The title bar shows 'ayoub@ip-172-31-35-39: ~'. The command 'sudo apt-get install apache2' is entered and highlighted with a red rectangular box. The output shows the package lists being read, the dependency tree being built, and the state information being read. It then lists additional packages to be installed, suggested packages, and new packages to be installed. The final line indicates that 0 packages are upgraded, 18 are newly installed, 0 are to be removed, and 0 are not upgraded. The total size of the archives to be downloaded is 9893 kB.

```
ayoub@ip-172-31-35-39:~$ sudo apt-get install apache2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils bzip2 libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap libgdbm-compat4 libjansson4
  liblua5.3-0 libperl5.32 mailcap mime-support perl perl-modules-5.32 ssl-cert
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser
  bzip2-doc perl-doc libterm-readline-gnu-perl | libterm-readline-perl-perl
  make libtap-harness-archive-perl
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils bzip2 libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap libgdbm-compat4 libjansson4
  liblua5.3-0 libperl5.32 mailcap mime-support perl perl-modules-5.32 ssl-cert
0 upgraded, 18 newly installed, 0 to remove and 0 not upgraded.
Need to get 9893 kB of archives.
```

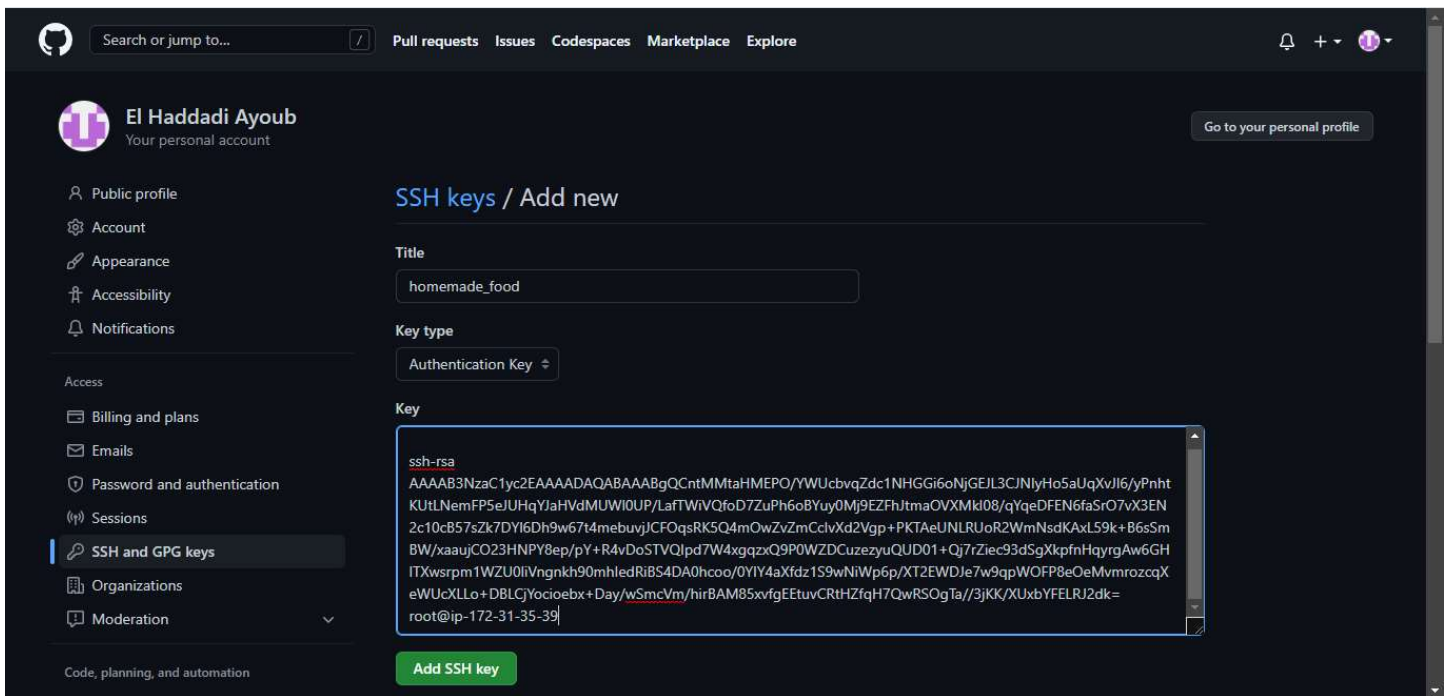
Après, nous devons installer Git afin de cloner notre site web qui existe dans GitHub, l'installation de Git se fait à travers la commande [sudo apt-get install git git-core](#).

```
ayoub@ip-172-31-35-39: ~  
ayoub@ip-172-31-35-39:~$ sudo apt-get install git git-core  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
Note, selecting 'git' instead of 'git-core'  
The following additional packages will be installed:  
  git-man liberror-perl patch  
Suggested packages:  
  git-daemon-run | git-daemon-sysvinit git-doc git-el git-email git-gui gitk  
  gitweb git-cvs git-mediawiki git-svn ed diffutils-doc  
The following NEW packages will be installed:  
  git git-man liberror-perl patch  
0 upgraded, 4 newly installed, 0 to remove and 0 not upgraded.  
Need to get 7514 kB of archives.  
After this operation, 38.2 MB of additional disk space will be used.  
Do you want to continue? [Y/n] Y  
Get:1 http://cdn-aws.deb.debian.org/debian bullseye/main amd64 liberror-perl all  
  0.17029-1 [31.0 kB]  
Get:2 http://cdn-aws.deb.debian.org/debian bullseye/main amd64 git-man all 1:2.3  
  0.2-1 [1827 kB]  
Get:3 http://cdn-aws.deb.debian.org/debian bullseye/main amd64 git amd64 1:2.30.  
  2-1 [5527 kB]  
Get:4 http://cdn-aws.deb.debian.org/debian bullseye/main amd64 patch amd64 2.7.6  
  -7 [128 kB]
```

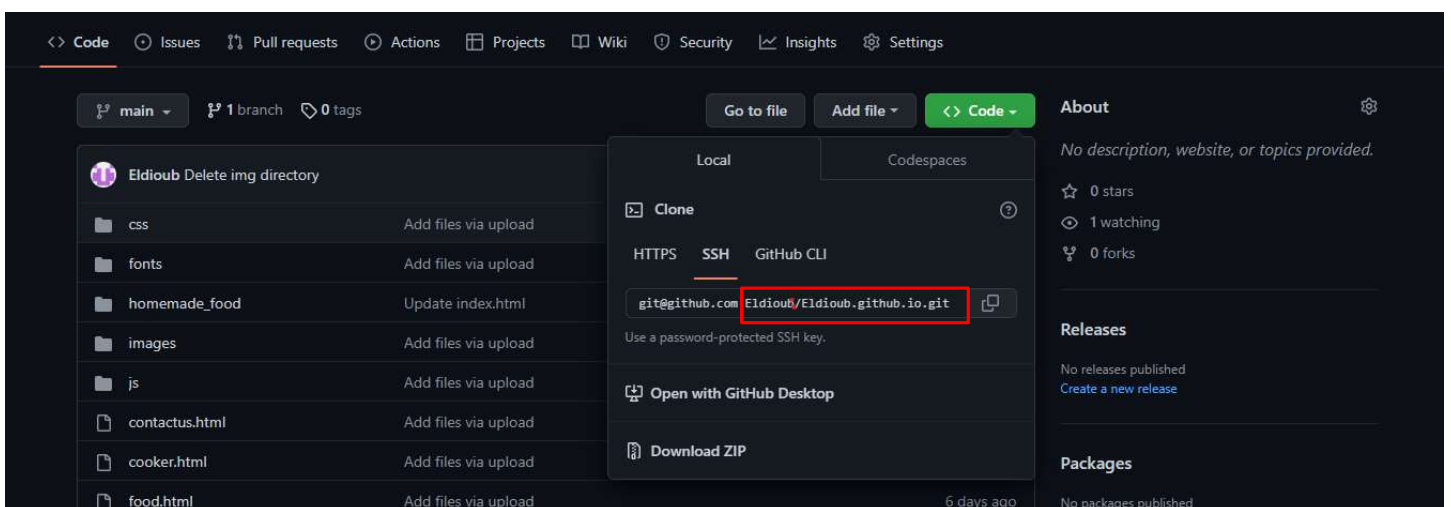
Nous allons lier le serveur web avec GitHub, pour cela, nous allons ajouter la clé publique de RSA de notre serveur dans les paramètres de GitHub, pour obtenir la clé publique de RSA du serveur, nous utiliserons la commande `cat ssh_host_rsa_key.pub`

```
ayoub@ip-172-31-35-39: /etc/ssh  
ayoub@ip-172-31-35-39:/etc/ssh$ cat ssh_host_rsa_key.pub  
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGCntMMtaHMEPO/YWUcbvq2dc1NHGGi6oNjGEJL3CJN  
IyHo5aUqXvJl6/yPnhtKUtLNemFP5eJUHqYJaHVdMUW10UP/LafTWiVQfoD7ZuPh6oBYuy0Mj9EZfHJ  
tmaOVXmkI08/qYqeDFEN6faSr07vX3EN2cl0cB57sZk7DYl6Dh9w67t4mebuvjJCFOqsRK5Q4mOwZvZ  
mCcIvXd2Vgp+PKTAeUNLRUoR2WmNsdKAXL59k+B6sSmBW/xaaujCO23HNPY8ep/pY+R4vDoSTVQIpd7  
W4xgqzxQ9P0WZDCuzezyuQUD01+Qj7rZiec93dSgXkpfnHqyrgAw6GH1TXwsrpmlWZU0liVngnkh90m  
hIedRiBS4DA0hcoo/0YIY4aXfdz1S9wNiWp6p/XT2EWDJe7w9qpWOFp8eOeMvmrozcgXeWUcXLLo+DB  
LCjYocioebx+Day/wSmcVm/nirBAM85xvfgEEtuvCRtHZfqH7QwRSOGTa//3jKK/XUxbYFELRJ2dk=  
root@ip-172-31-35-39
```

Après l'obtention de la clé publique de RSA du serveur, nous allons l'ajouter dans la partie indiquée ci-dessous.



Maintenant, nous allons prendre le chemin encadré en rouge dans l'image au-dessous.



Et nous allons cloner le site web à partir GitHub via la commande `sudo git clone https://github.com/ssh_link`

```
ayoub@ip-172-31-35-39:/var/www/html$ sudo git clone https://github.com/Eldioub/  
Eldioub.github.io.git  
Cloning into 'Eldioub.github.io'...  
remote: Enumerating objects: 589, done.  
remote: Counting objects: 100% (47/47), done.  
remote: Compressing objects: 100% (30/30), done.  
remote: Total 589 (delta 21), reused 35 (delta 15), pack-reused 542  
Receiving objects: 100% (589/589), 14.54 MiB | 22.73 MiB/s, done.  
Resolving deltas: 100% (227/227), done.
```

Maintenant, nous allons ouvrir un navigateur web, nous allons taper l'adresse IP publique de notre serveur web et nous observerons que le site web est bien cloné.

