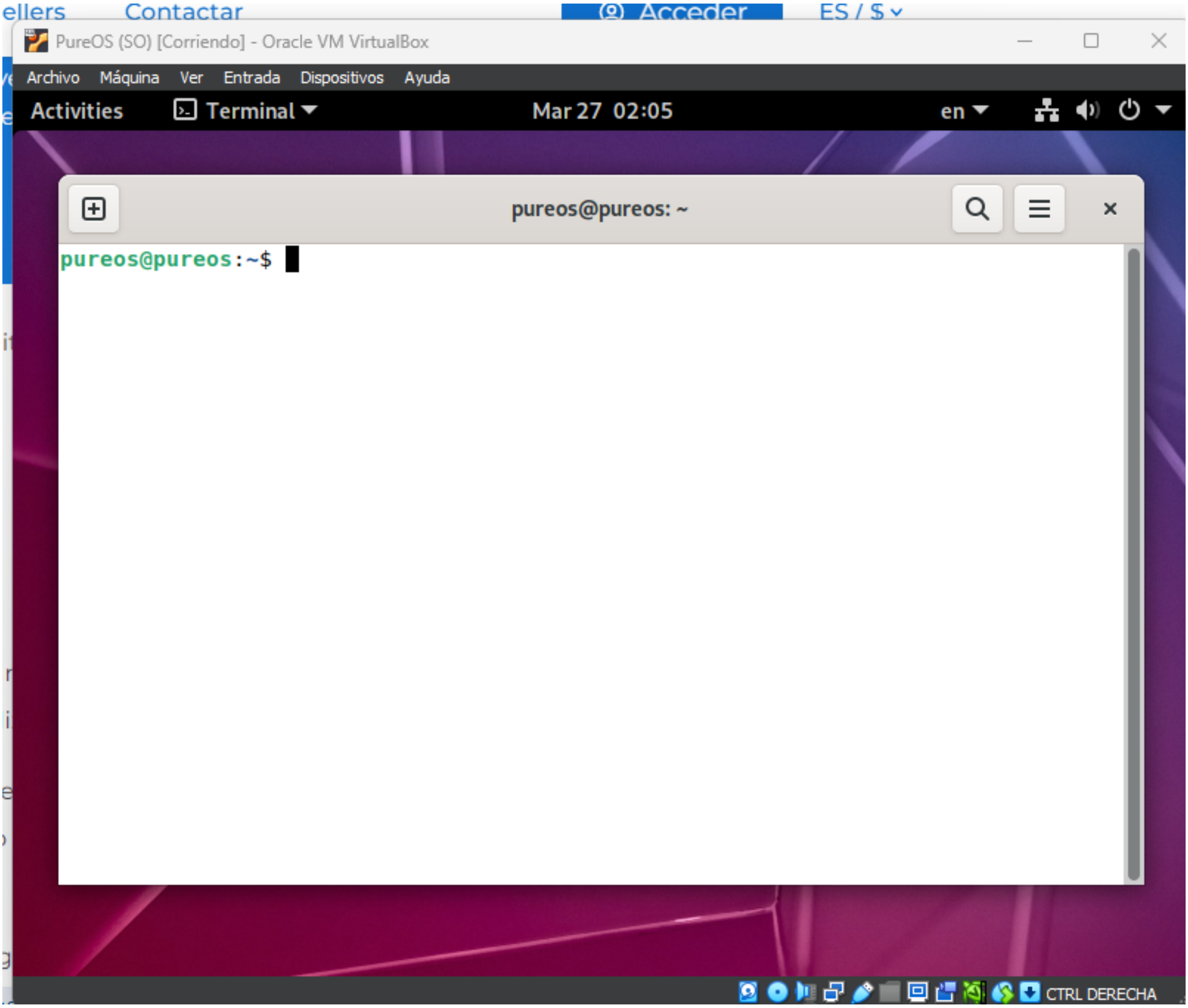
Certificado NGINX

En este proyecto veremos como obtener un certificado con NGINX autofirmado para la clase de seguridad informatica - Electiva VI

Presentado por: Brahyam Hurtado Quiceno

Instalacion de PureOS

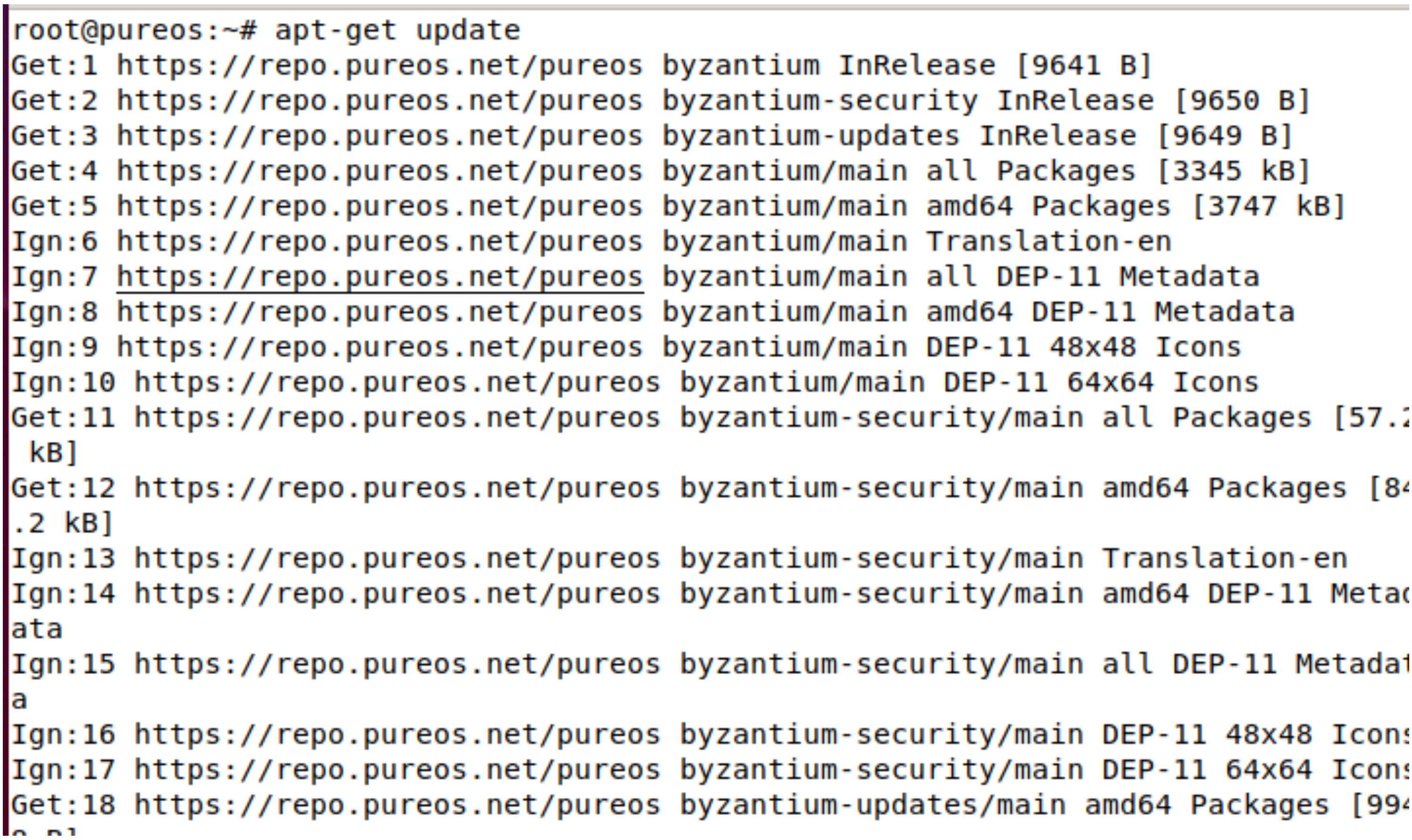
Para poder usar este certificado necestimos el sistema operatico de PureOS


PureOS (SO) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Activities
Terminal
Mar 27 02:05
en
pureos@pureos: ~
CTRL DERECHA

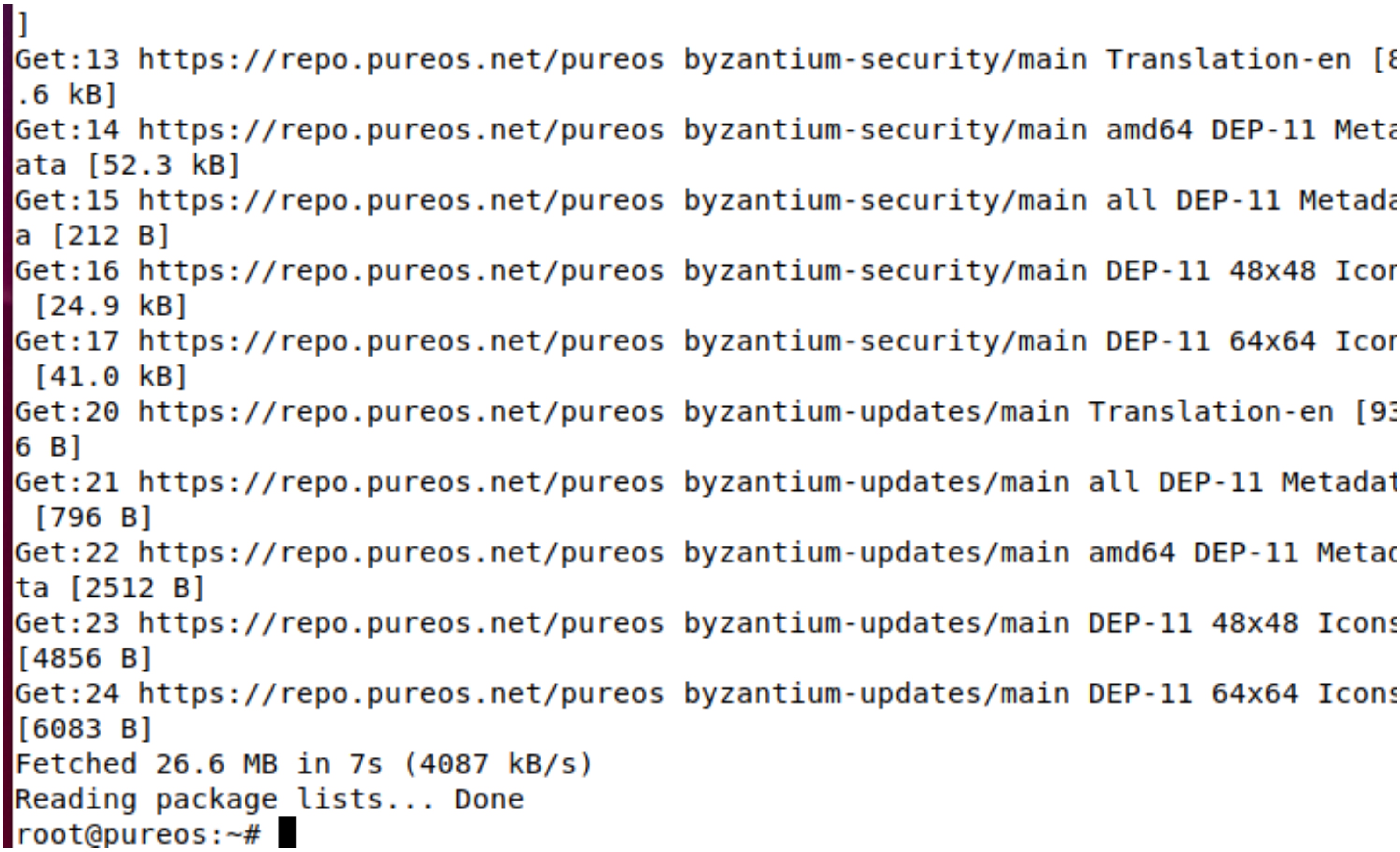
```
pureos@pureos:~$
```

Instalacion NGINX

Ahora hacemos la instalacion de NGINX en PureOS, hacemos actualizacion de paqueteria

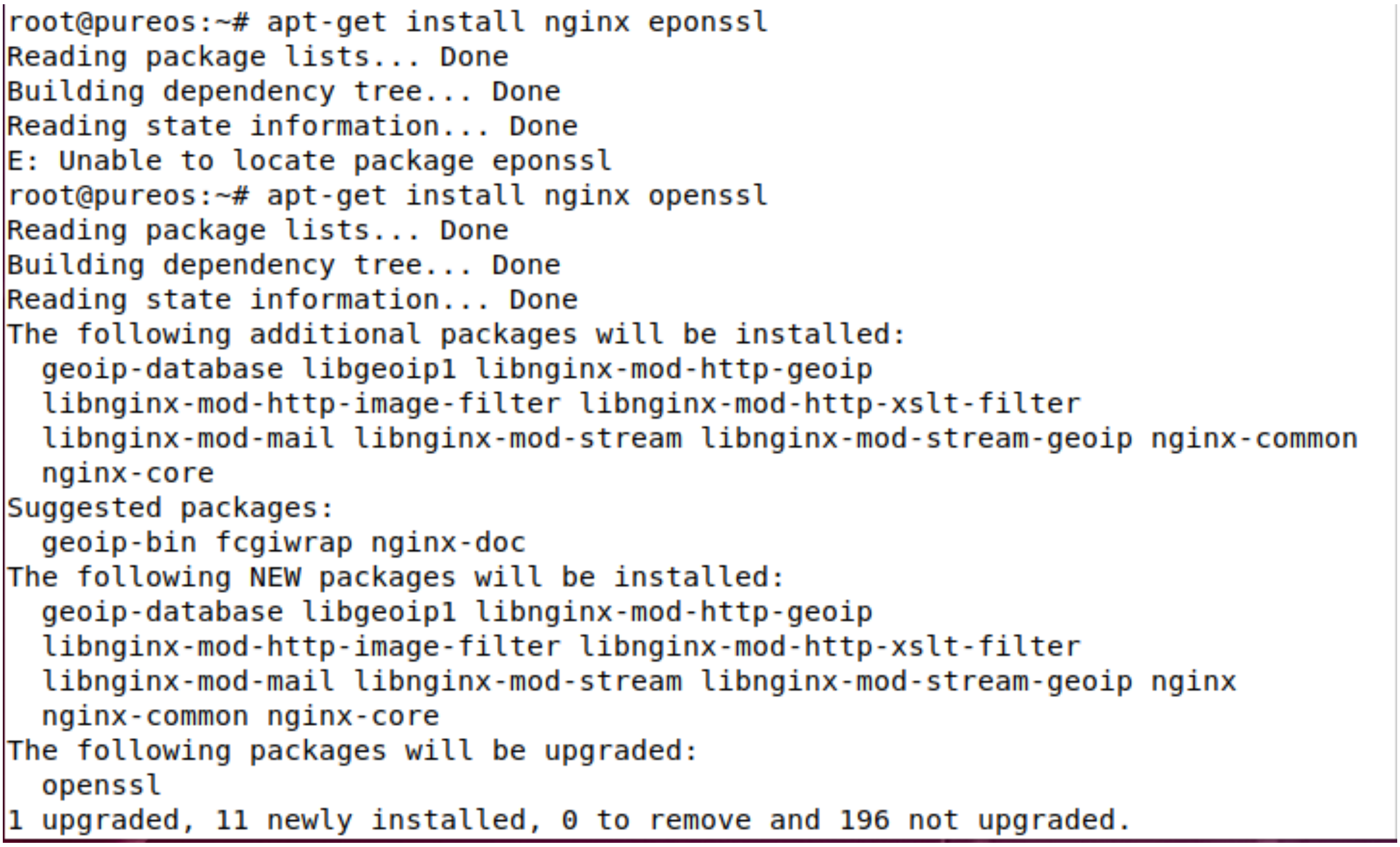


```
root@pureos:~# apt-get update
Get:1 https://repo.pureos.net/pureos byzantium InRelease [9641 B]
Get:2 https://repo.pureos.net/pureos byzantium-security InRelease [9650 B]
Get:3 https://repo.pureos.net/pureos byzantium-updates InRelease [9649 B]
Get:4 https://repo.pureos.net/pureos byzantium/main all Packages [3345 kB]
Get:5 https://repo.pureos.net/pureos byzantium/main amd64 Packages [3747 kB]
Ign:6 https://repo.pureos.net/pureos byzantium/main Translation-en
Ign:7 https://repo.pureos.net/pureos byzantium/main all DEP-11 Metadata
Ign:8 https://repo.pureos.net/pureos byzantium/main amd64 DEP-11 Metadata
Ign:9 https://repo.pureos.net/pureos byzantium/main DEP-11 48x48 Icons
Ign:10 https://repo.pureos.net/pureos byzantium/main DEP-11 64x64 Icons
Get:11 https://repo.pureos.net/pureos byzantium-security/main all Packages [57.
 kB]
Get:12 https://repo.pureos.net/pureos byzantium-security/main amd64 Packages [8
.2 kB]
Ign:13 https://repo.pureos.net/pureos byzantium-security/main Translation-en
Ign:14 https://repo.pureos.net/pureos byzantium-security/main amd64 DEP-11 Meta
ata
Ign:15 https://repo.pureos.net/pureos byzantium-security/main all DEP-11 Metada
a
Ign:16 https://repo.pureos.net/pureos byzantium-security/main DEP-11 48x48 Icon
Ign:17 https://repo.pureos.net/pureos byzantium-security/main DEP-11 64x64 Icon
Get:18 https://repo.pureos.net/pureos byzantium-updates/main amd64 Packages [99
```

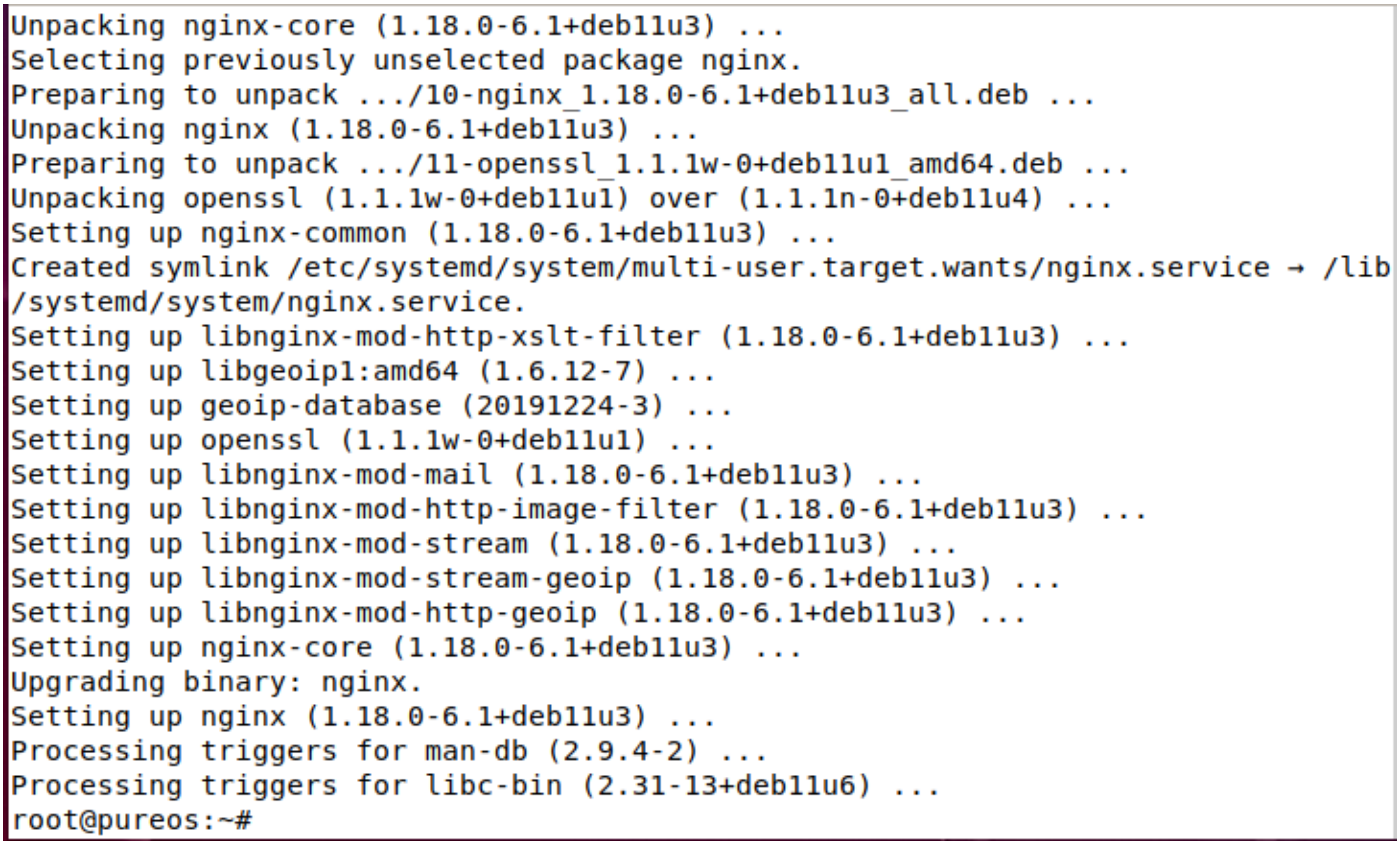


```
]
Get:13 https://repo.pureos.net/pureos byzantium-security/main Translation-en [
.6 kB]
Get:14 https://repo.pureos.net/pureos byzantium-security/main amd64 DEP-11 Meta
ata [52.3 kB]
Get:15 https://repo.pureos.net/pureos byzantium-security/main all DEP-11 Metada
a [212 B]
Get:16 https://repo.pureos.net/pureos byzantium-security/main DEP-11 48x48 Icor
 [24.9 kB]
Get:17 https://repo.pureos.net/pureos byzantium-security/main DEP-11 64x64 Icor
 [41.0 kB]
Get:20 https://repo.pureos.net/pureos byzantium-updates/main Translation-en [93
6 B]
Get:21 https://repo.pureos.net/pureos byzantium-updates/main all DEP-11 Metadat
 [796 B]
Get:22 https://repo.pureos.net/pureos byzantium-updates/main amd64 DEP-11 Metac
ta [2512 B]
Get:23 https://repo.pureos.net/pureos byzantium-updates/main DEP-11 48x48 Icons
[4856 B]
Get:24 https://repo.pureos.net/pureos byzantium-updates/main DEP-11 64x64 Icons
[6083 B]
Fetched 26.6 MB in 7s (4087 kB/s)
Reading package lists... Done
root@pureos:~# █
```

Y ahora podemos hacer la instalacion de NGINX



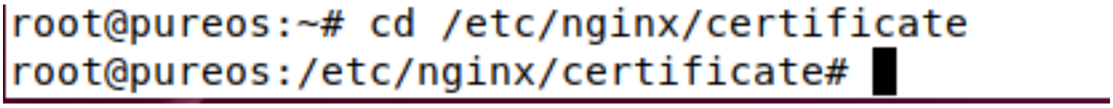
```
root@pureos:~# apt-get install nginx eponssl
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
E: Unable to locate package eponssl
root@pureos:~# apt-get install nginx openssl
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  geoip-database libgeoip1 libnginx-mod-http-geoip
  libnginx-mod-http-image-filter libnginx-mod-http-xslt-filter
  libnginx-mod-mail libnginx-mod-stream libnginx-mod-stream-geoip nginx-common
  nginx-core
Suggested packages:
  geoip-bin fcgiwrap nginx-doc
The following NEW packages will be installed:
  geoip-database libgeoip1 libnginx-mod-http-geoip
  libnginx-mod-http-image-filter libnginx-mod-http-xslt-filter
  libnginx-mod-mail libnginx-mod-stream libnginx-mod-stream-geoip nginx
  nginx-common nginx-core
The following packages will be upgraded:
  openssl
1 upgraded, 11 newly installed, 0 to remove and 196 not upgraded.
```



```
Unpacking nginx-core (1.18.0-6.1+deb11u3) ...
Selecting previously unselected package nginx.
Preparing to unpack .../10-nginx_1.18.0-6.1+deb11u3_all.deb ...
Unpacking nginx (1.18.0-6.1+deb11u3) ...
Preparing to unpack .../11-openssl_1.1.1w-0+deb11u1_amd64.deb ...
Unpacking openssl (1.1.1w-0+deb11u1) over (1.1.1n-0+deb11u4) ...
Setting up nginx-common (1.18.0-6.1+deb11u3) ...
Created symlink /etc/systemd/system/multi-user.target.wants/nginx.service → /lib
/systemd/system/nginx.service.
Setting up libnginx-mod-http-xslt-filter (1.18.0-6.1+deb11u3) ...
Setting up libgeoip1:amd64 (1.6.12-7) ...
Setting up geoip-database (20191224-3) ...
Setting up openssl (1.1.1w-0+deb11u1) ...
Setting up libnginx-mod-mail (1.18.0-6.1+deb11u3) ...
Setting up libnginx-mod-http-image-filter (1.18.0-6.1+deb11u3) ...
Setting up libnginx-mod-stream (1.18.0-6.1+deb11u3) ...
Setting up libnginx-mod-stream-geoip (1.18.0-6.1+deb11u3) ...
Setting up libnginx-mod-http-geoip (1.18.0-6.1+deb11u3) ...
Setting up nginx-core (1.18.0-6.1+deb11u3) ...
Upgrading binary: nginx.
Setting up nginx (1.18.0-6.1+deb11u3) ...
Processing triggers for man-db (2.9.4-2) ...
Processing triggers for libc-bin (2.31-13+deb11u6) ...
root@pureos:~#
```

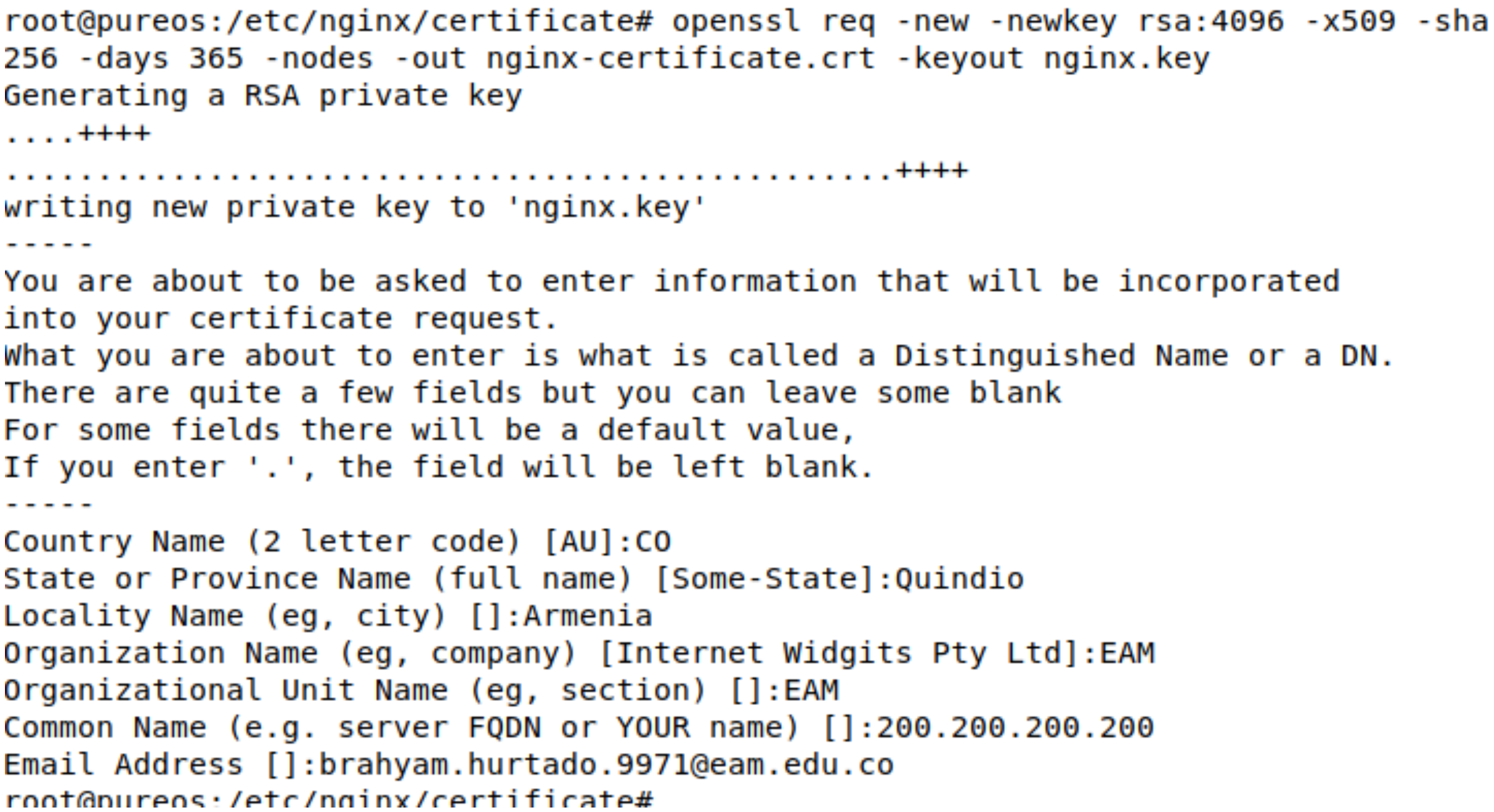
Creacion de Llave con SSL

Primero nos dirigimos al paquete donde encontramos el certificado



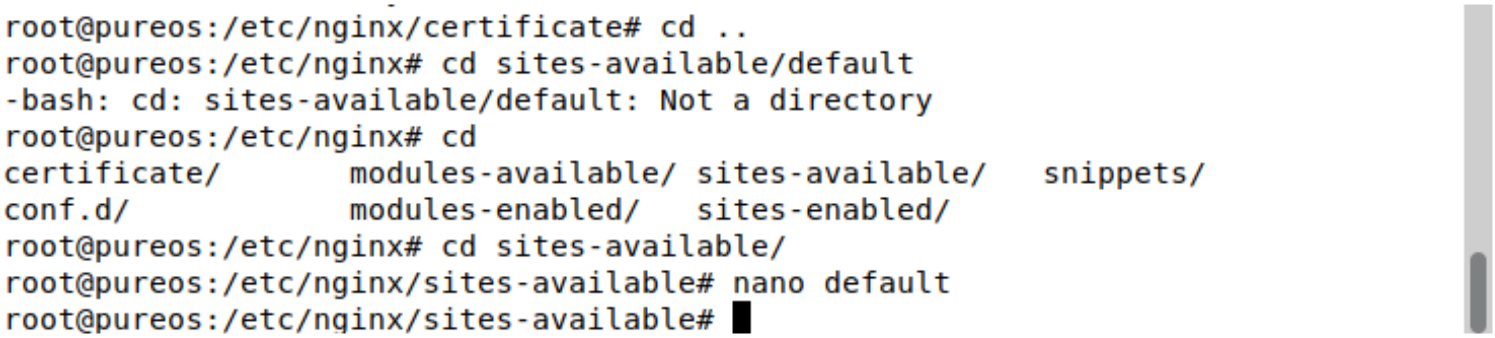
```
root@pureos:~# cd /etc/nginx/certificate
root@pureos:/etc/nginx/certificate# 
```

Y aqui usamos el comando de openSSL



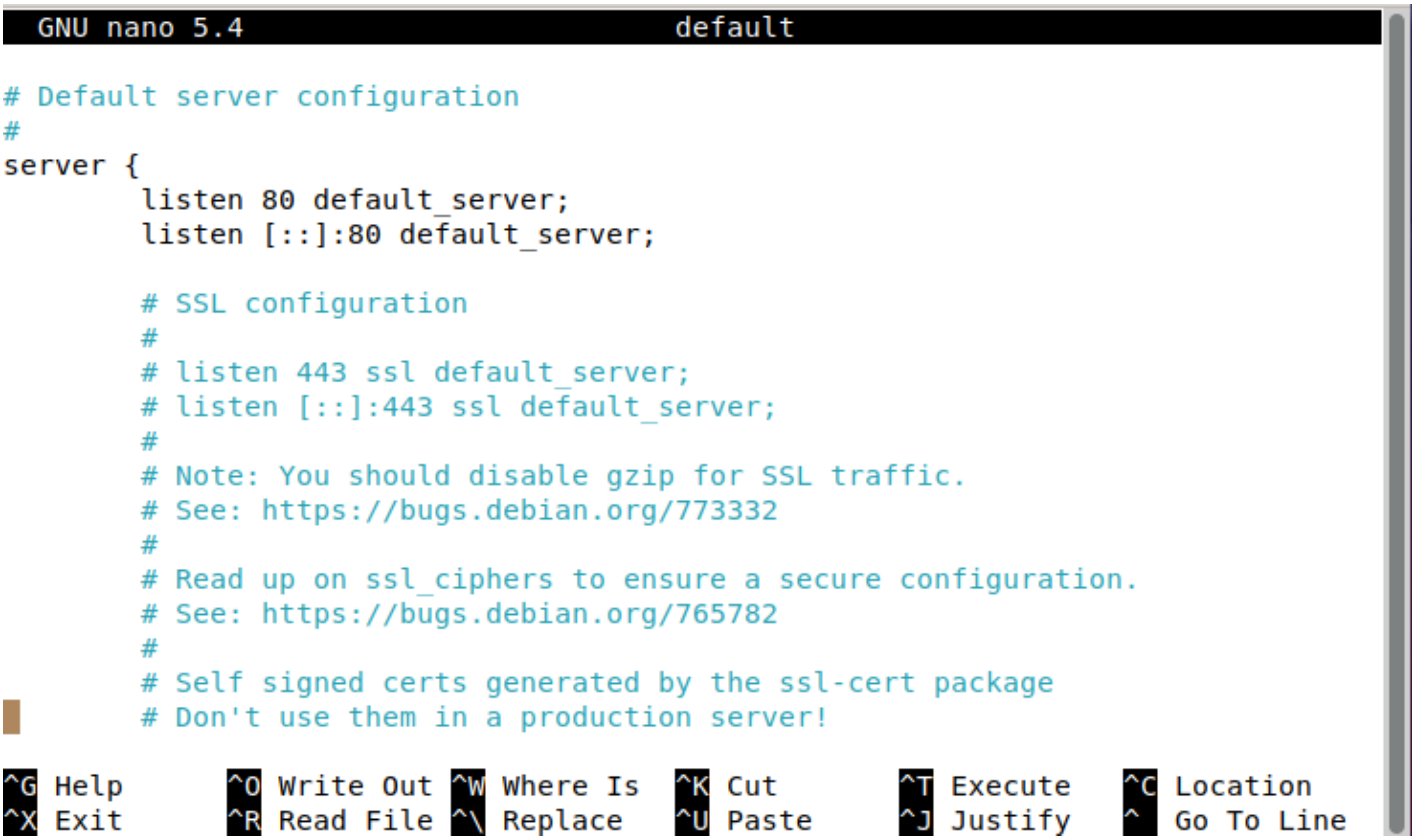
```
root@pureos:/etc/nginx/certificate# openssl req -new -newkey rsa:4096 -x509 -sha
256 -days 365 -nodes -out nginx-certificate.crt -keyout nginx.key
Generating a RSA private key
....++++
................................................++++
writing new private key to 'nginx.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CO
State or Province Name (full name) [Some-State]:Quindio
Locality Name (eg, city) []:Armenia
Organization Name (eg, company) [Internet Widgits Pty Ltd]:EAM
Organizational Unit Name (eg, section) []:EAM
Common Name (e.g. server FQDN or YOUR name) []:200.200.200.200
Email Address []:brahyam.hurtado.9971@eam.edu.co
root@pureos:/etc/nginx/certificate#
```

Ahora debemos editar el archivo de configuracion de NGINX



```
root@pureos:/etc/nginx/certificate# cd ..
root@pureos:/etc/nginx# cd sites-available/default
-bash: cd: sites-available/default: Not a directory
root@pureos:/etc/nginx# cd
certificate/       modules-available/ sites-available/   snippets/
conf.d/            modules-enabled/   sites-enabled/
root@pureos:/etc/nginx# cd sites-available/
root@pureos:/etc/nginx/sites-available# nano default
root@pureos:/etc/nginx/sites-available# 
```

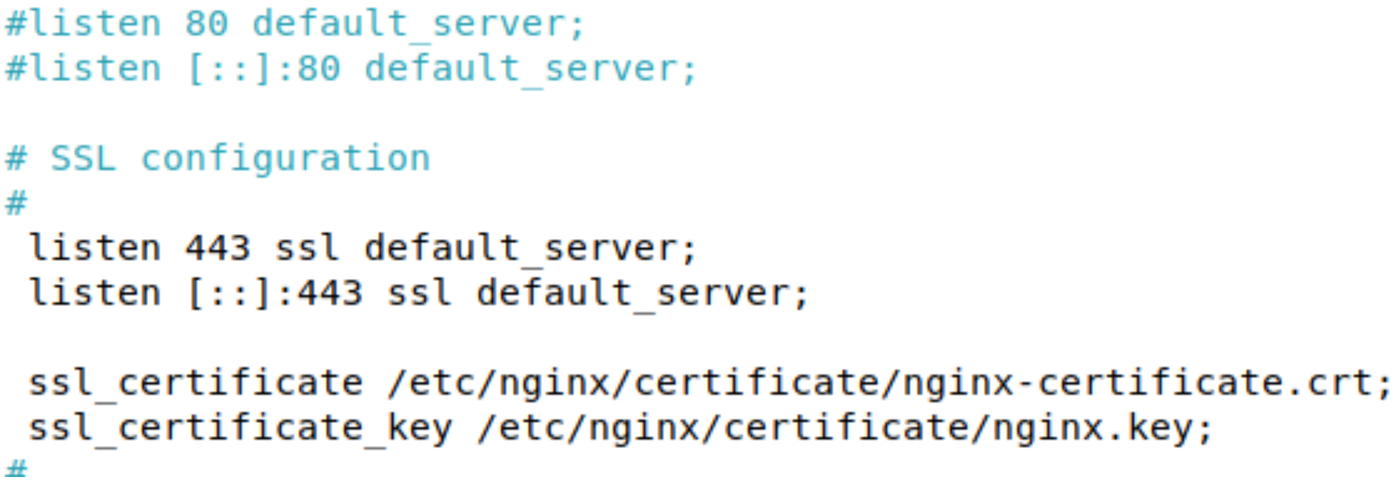
y aqui podremos acceder al archivo default



```
# Default server configuration
#
server {
        listen 80 default_server;
        listen [::]:80 default_server;

        # SSL configuration
        #
        # listen 443 ssl default_server;
        # listen [::]:443 ssl default_server;
        #
        # Note: You should disable gzip for SSL traffic.
        # See: https://bugs.debian.org/773332
        #
        # Read up on ssl_ciphers to ensure a secure configuration.
        # See: https://bugs.debian.org/765782
        #
        # Self signed certs generated by the ssl-cert package
        # Don't use them in a production server!
```

Luego empezamos la modificacion de el archivo, comenzamos por comentar el default server y descomentar la linea de puerto 443 y agregar las lineas de la ubicacion de el certificado y la llave



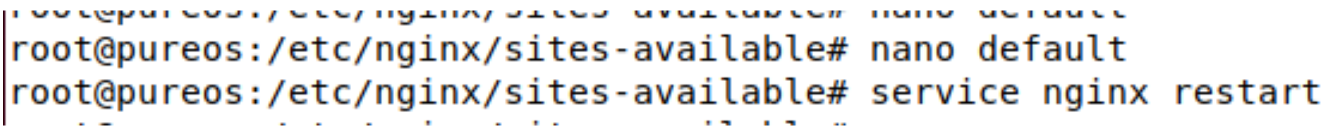
```
#listen 80 default_server;
#listen [::]:80 default_server;

# SSL configuration
#
 listen 443 ssl default_server;
 listen [::]:443 ssl default_server;

 ssl_certificate /etc/nginx/certificate/nginx-certificate.crt;
 ssl_certificate_key /etc/nginx/certificate/nginx.key;
#
```

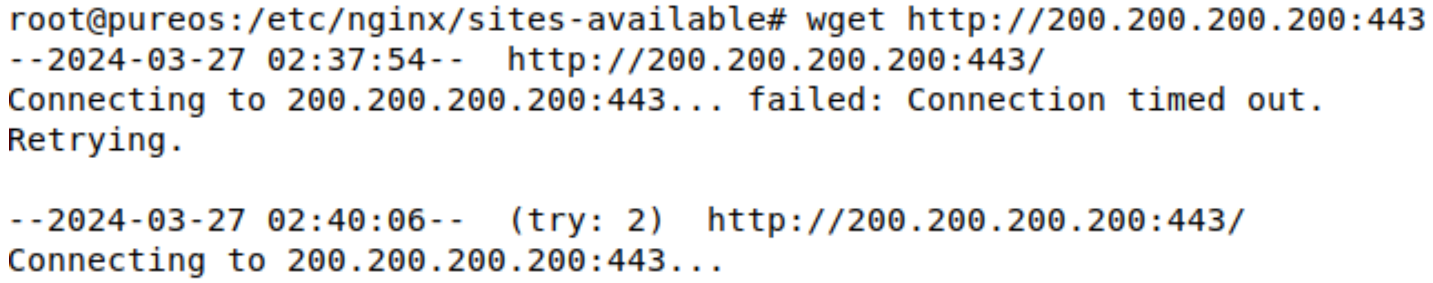
Luego sobreescribimos el archivo y salimos con ctrl+x

En este paso debemos reiniciar el servicio de NGINX



```
root@pureos:/etc/nginx/sites-available# nano default
root@pureos:/etc/nginx/sites-available# service nginx restart
```

Y ahora debemos acceder a nuestra URL para comprobar el servicio



```
root@pureos:/etc/nginx/sites-available# wget http://200.200.200.200:443
--2024-03-27 02:37:54--  http://200.200.200.200:443/
Connecting to 200.200.200.200:443... failed: Connection timed out.
Retrying.

--2024-03-27 02:40:06--  (try: 2)  http://200.200.200.200:443/
Connecting to 200.200.200.200:443...
```