



**UNIVERSIDAD AUTÓNOMA DE CHIAPAS**

**LICENCIATURA EN INGENIERIA EN DESARROLLO  
Y TECNOLOGIAS DE SOFTWARE**



# **ANALISIS DE VULNERABILIDADES**

## **Actividad 3.3**

Nombre del alumno: Luis Gerardo Mendoza Gomez | A200004

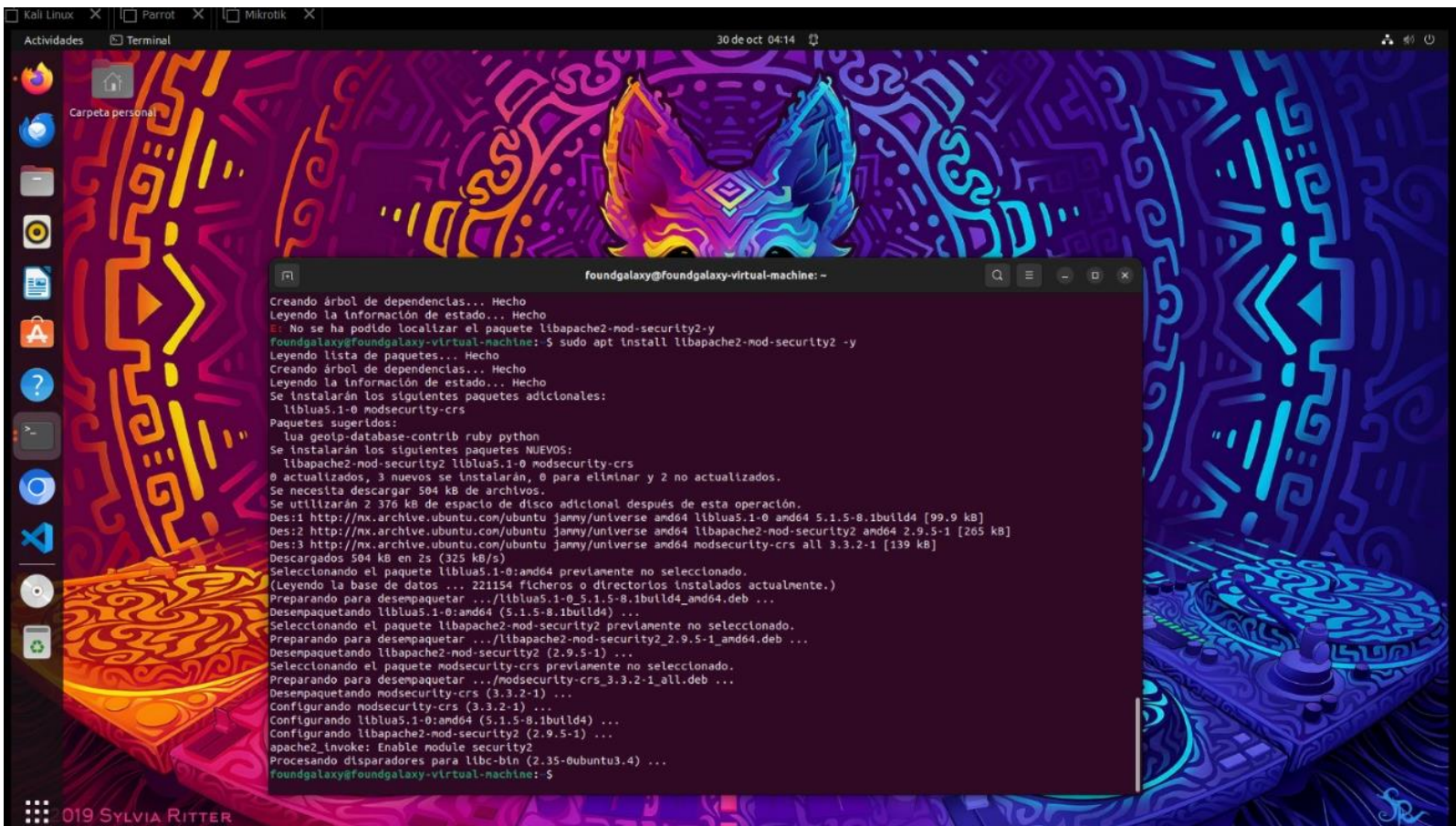
Nombre del catedrático: Dr. Luis Gutiérrez Alfaro

Semestre: 7

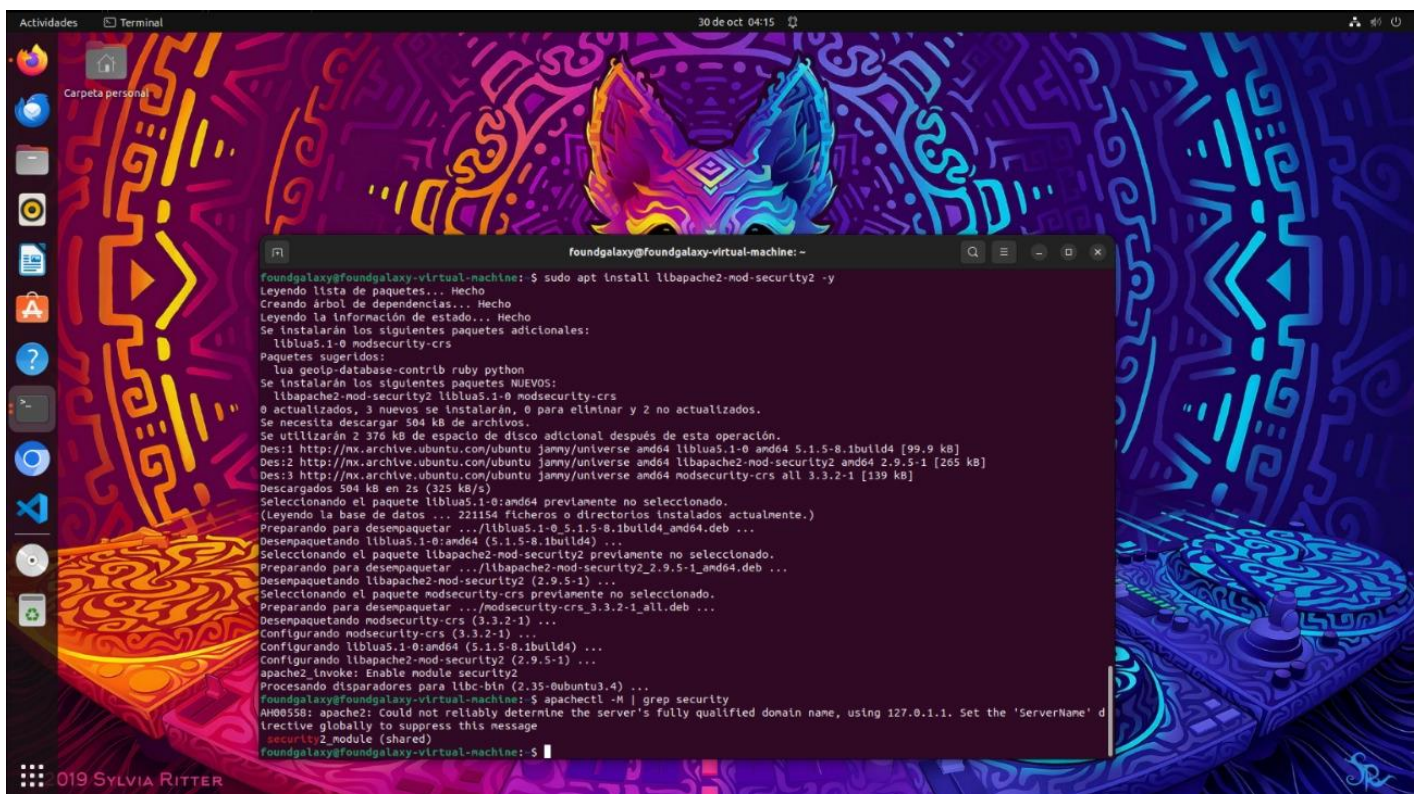
Grupo: M

Fecha de entrega: 11/11/23

# Instalación del WAF (ModSecurity)

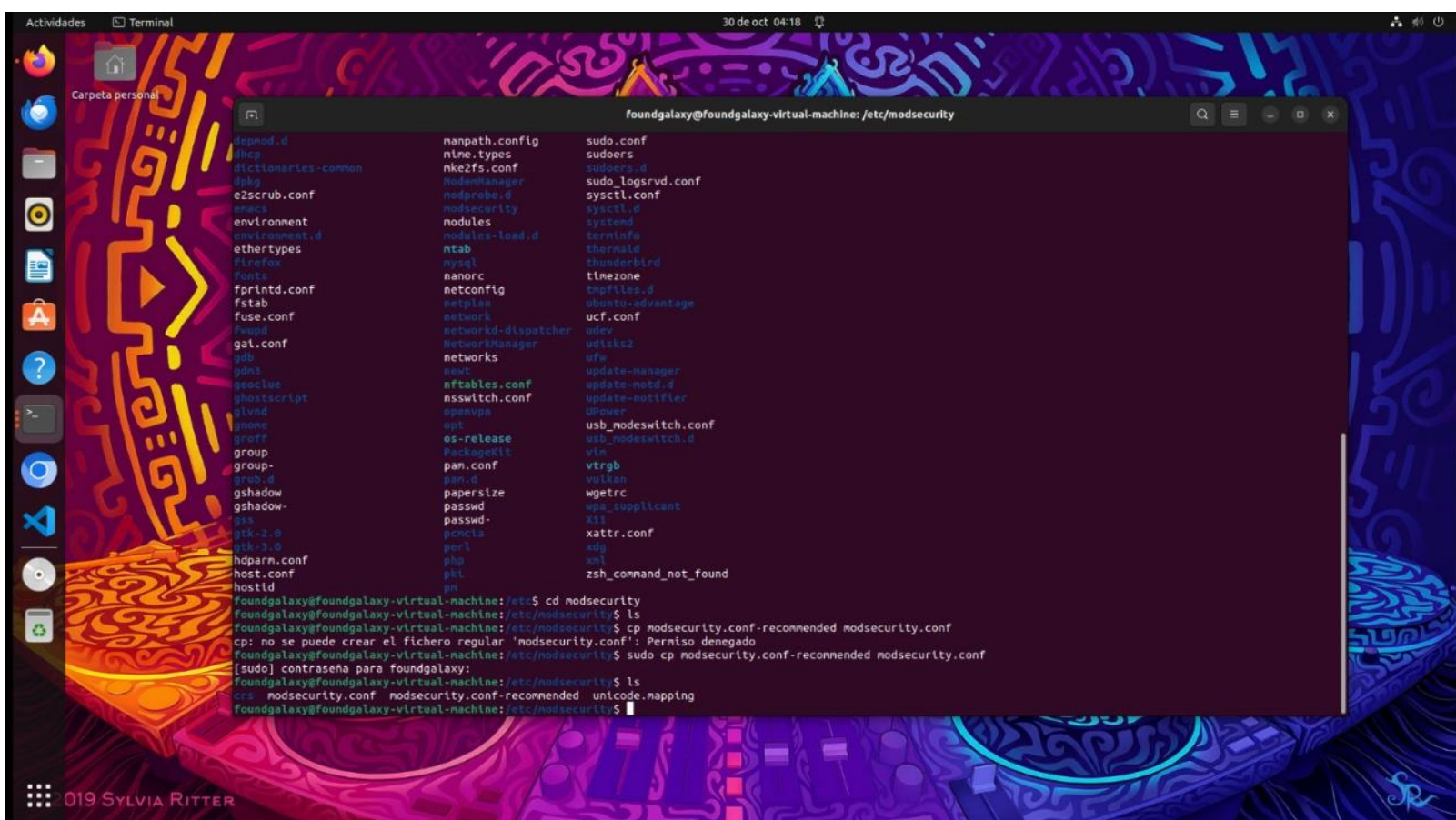


## Instalación de la librería de ModSecurity

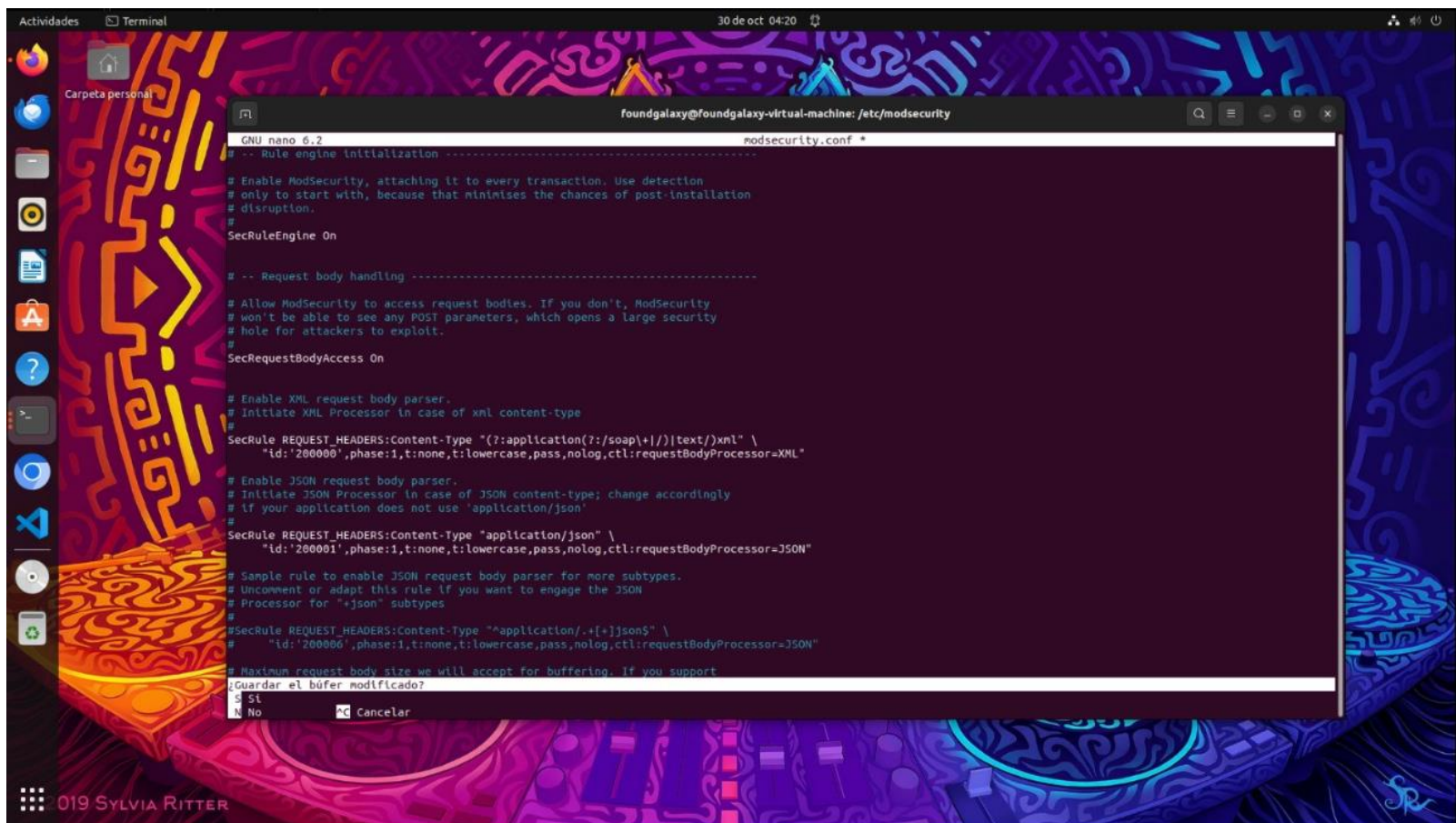


Verificamos que ModSecurity se instalo correctamente.

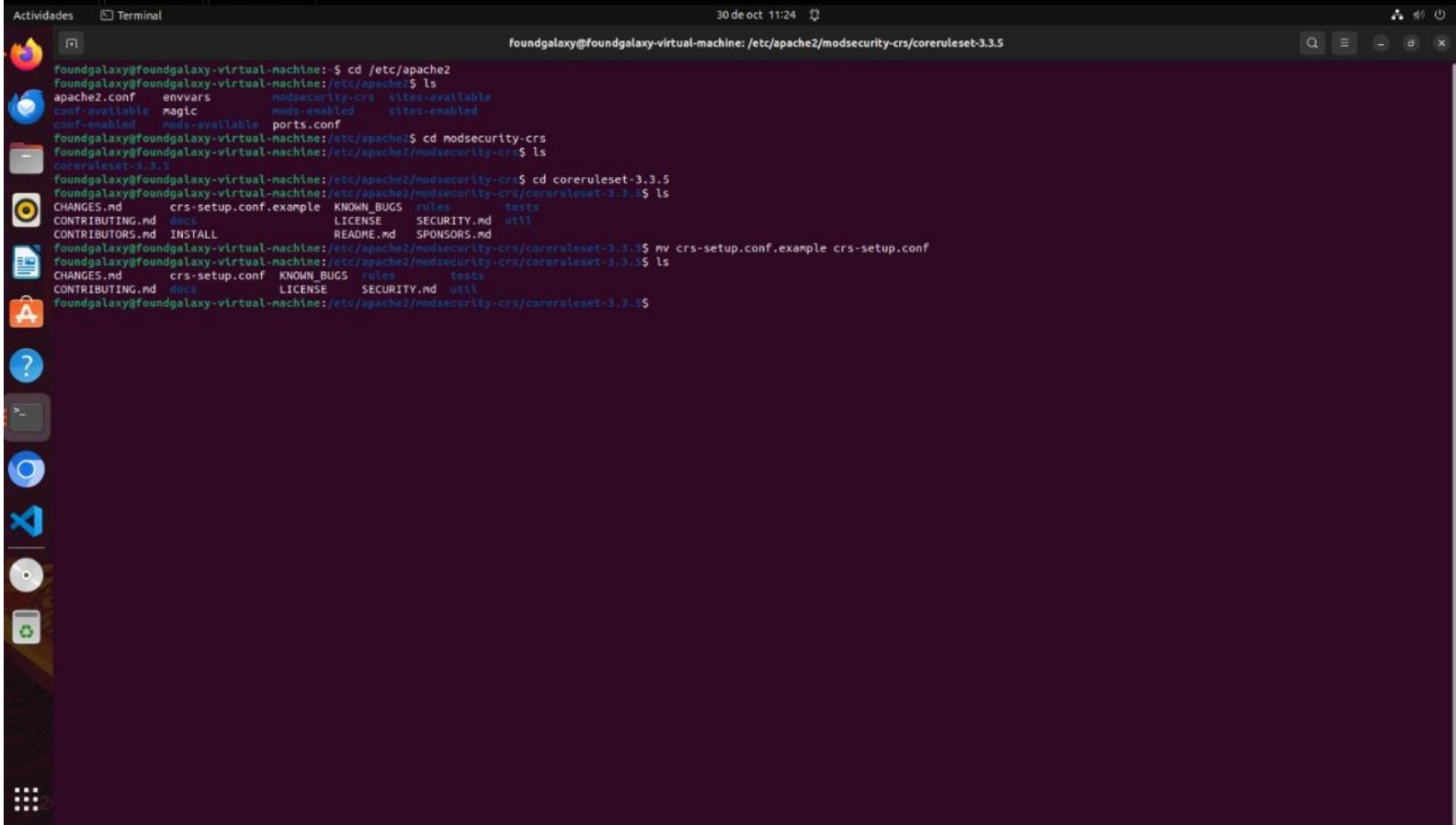




Hacemos una copia de seguridad del archivo modsecurity.conf-recommended en la ruta /etc/modsecurity y en la cual trabajaremos enseguida.

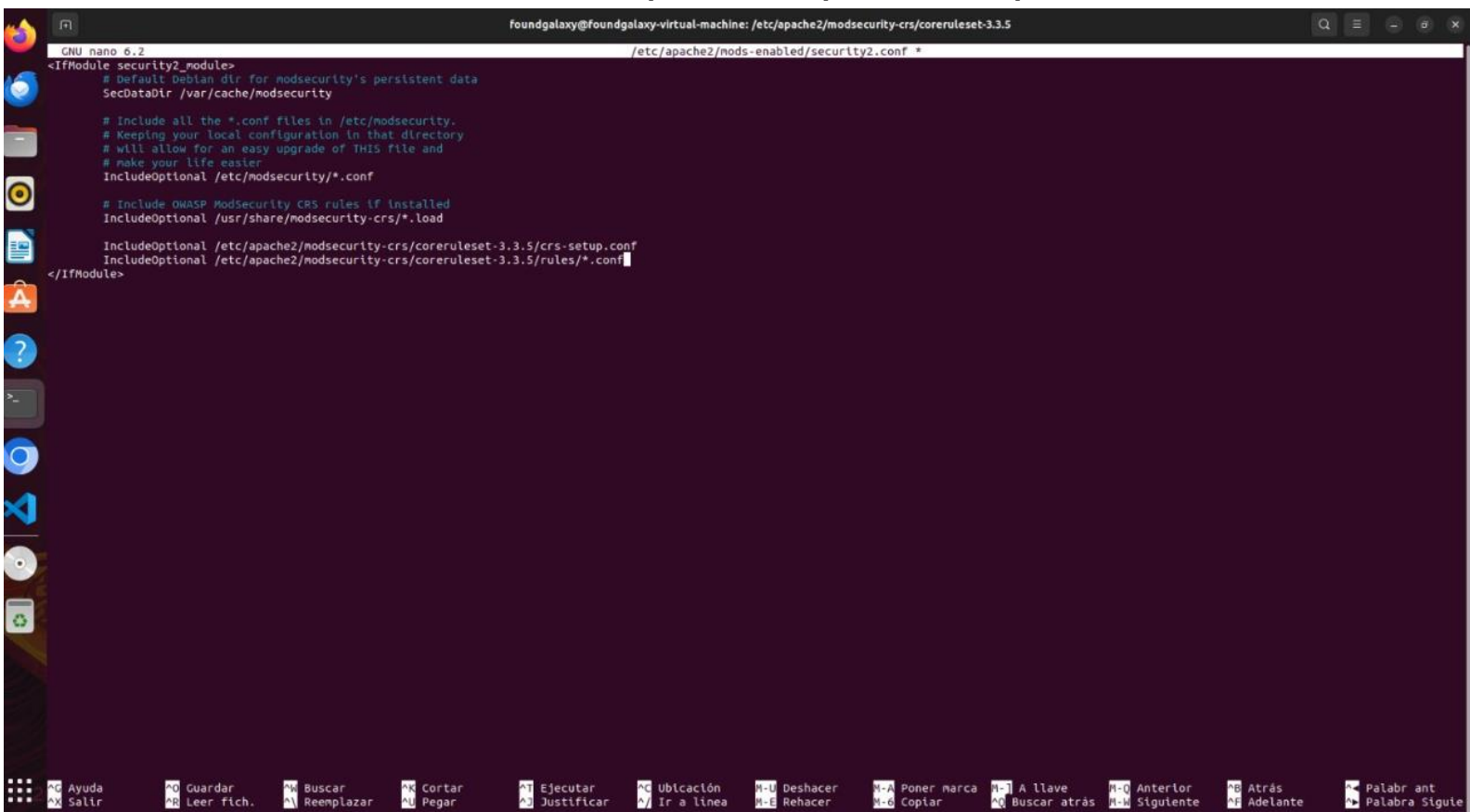


Configuramos el archivo modsecurity.conf quedando de la forma como muestra la captura de arriba y guardamos los cambios.



```
foundgalaxy@foundgalaxy-virtual-machine: /etc/apache2/modsecurity-crs/coreruleset-3.3.5
foundgalaxy@foundgalaxy-virtual-machine:~$ cd /etc/apache2
foundgalaxy@foundgalaxy-virtual-machine:/etc/apache2$ ls
apache2.conf  envvars      modsecurity-crs  sites-available
conf-available  magic        mods-enabled     sites-enabled
conf-enabled   mods-available  ports.conf
foundgalaxy@foundgalaxy-virtual-machine:/etc/apache2$ cd modsecurity-crs
foundgalaxy@foundgalaxy-virtual-machine:/etc/apache2/modsecurity-crs$ ls
coreruleset-3.3.5
foundgalaxy@foundgalaxy-virtual-machine:/etc/apache2/modsecurity-crs$ cd coreruleset-3.3.5
foundgalaxy@foundgalaxy-virtual-machine:/etc/apache2/modsecurity-crs/coreruleset-3.3.5$ ls
CHANGES.md  crs-setup.conf.example  KNOWN_BUGS  rules      tests
CONTRIBUTING.md  docs                    LICENSE      SECURITY.md  util
CONTRIBUTORS.md  INSTALL                README.md    SPONSORS.md
foundgalaxy@foundgalaxy-virtual-machine:/etc/apache2/modsecurity-crs/coreruleset-3.3.5$ mv crs-setup.conf.example crs-setup.conf
foundgalaxy@foundgalaxy-virtual-machine:/etc/apache2/modsecurity-crs/coreruleset-3.3.5$ ls
CHANGES.md  crs-setup.conf  KNOWN_BUGS  rules      tests
CONTRIBUTING.md  docs          LICENSE      SECURITY.md  util
foundgalaxy@foundgalaxy-virtual-machine:/etc/apache2/modsecurity-crs/coreruleset-3.3.5$
```

Descargamos las CoreRules en su ultima versión para ModSecurity y renombramos el archivo crs-setup-conf.example a crs-setup.conf



```
GNU nano 6.2 /etc/apache2/mods-enabled/security2.conf *
<IfModule security2_module>
    # Default Debian dir for modsecurity's persistent data
    SecDataDir /var/cache/modsecurity

    # Include all the *.conf files in /etc/modsecurity.
    # Keeping your local configuration in that directory
    # will allow for an easy upgrade of THIS file and
    # make your life easier
    IncludeOptional /etc/modsecurity/*.conf

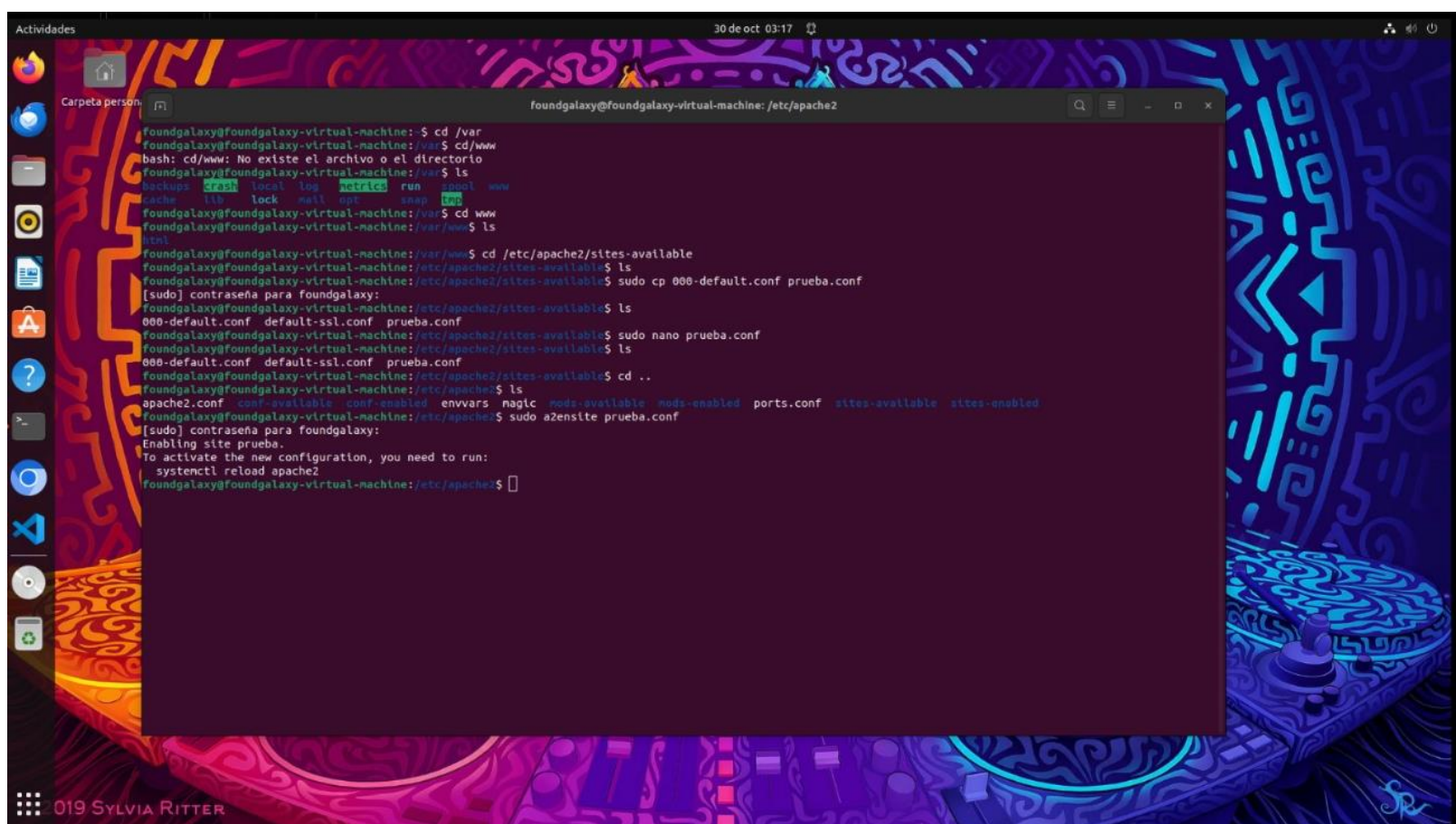
    # Include OWASP ModSecurity CRS rules if installed
    IncludeOptional /usr/share/modsecurity-crs/*.load

    IncludeOptional /etc/apache2/modsecurity-crs/coreruleset-3.3.5/crs-setup.conf
    IncludeOptional /etc/apache2/modsecurity-crs/coreruleset-3.3.5/rules/*.conf
</IfModule>
```

Editamos el archivo security2.conf para que quede configurado de la forma que muestra la captura anterior.



# Configuración del VirtualHost para redireccionamiento de http a https



```
foundgalaxy@foundgalaxy-virtual-machine: /etc/apache2
foundgalaxy@foundgalaxy-virtual-machine:~$ cd /var
foundgalaxy@foundgalaxy-virtual-machine:~$ cd /www
bash: cd /www: No existe el archivo o el directorio
foundgalaxy@foundgalaxy-virtual-machine:~$ ls
backups  cron  local  log  metrics  run  snap  www
cache  lib  lock  mail  opt  snap  tmp
foundgalaxy@foundgalaxy-virtual-machine:~$ cd /www
foundgalaxy@foundgalaxy-virtual-machine:~$ ls
html
foundgalaxy@foundgalaxy-virtual-machine:~$ cd /etc/apache2/sites-available
foundgalaxy@foundgalaxy-virtual-machine:~$ ls
000-default.conf  default-ssl.conf  prueba.conf
foundgalaxy@foundgalaxy-virtual-machine:~$ sudo cp 000-default.conf prueba.conf
[sudo] contraseña para foundgalaxy:
foundgalaxy@foundgalaxy-virtual-machine:~$ ls
000-default.conf  default-ssl.conf  prueba.conf
foundgalaxy@foundgalaxy-virtual-machine:~$ sudo nano prueba.conf
foundgalaxy@foundgalaxy-virtual-machine:~$ ls
000-default.conf  default-ssl.conf  prueba.conf
foundgalaxy@foundgalaxy-virtual-machine:~$ cd ..
foundgalaxy@foundgalaxy-virtual-machine:~$ ls
apache2.conf  conf-available  conf-enabled  envvars  magic  mods-available  mods-enabled  ports.conf  sites-available  sites-enabled
foundgalaxy@foundgalaxy-virtual-machine:~$ sudo a2ensite prueba.conf
[sudo] contraseña para foundgalaxy:
Enabling site prueba.
To activate the new configuration, you need to run:
systemctl reload apache2
foundgalaxy@foundgalaxy-virtual-machine:~$
```

Dentro de la ruta “/etc/apache2/sites-available” realizamos una copia del archivo 000-default.conf y lo nombramos como queramos, en este caso se nombro “prueba.conf” y usamos el comando “a2ensite \*archivo .conf que previamente le hicimos una copia\*” para habilitarlo.

```
foundgalaxy@foundgalaxy-virtual-machine: /etc/apache2/sites-available
GNU nano 6.2 prueba.conf *
<VirtualHost *:80>
# The ServerName directive sets the request scheme, hostname and port that
# the server uses to identify itself. This is used when creating
# redirection URLs. In the context of virtual hosts, the ServerName
# specifies what hostname must appear in the request's Host: header to
# match this virtual host. For the default virtual host (this file) this
# value is not decisive as it is used as a last resort host regardless.
# However, you must set it for any further virtual host explicitly.
ServerName foundgalaxy.com

ServerAdmin webmaster@localhost
DocumentRoot /var/www/html/DVWA
Redirect / https://foundgalaxy.com/DVWA

<Directory /var/www/html/DVWA>
Options FollowSymLinks
AllowOverride All
Require all granted
</Directory>

# Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
# error, crit, alert, emerg.
# It is also possible to configure the loglevel for particular
# modules, e.g.
#LogLevel info ssl:warn

ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined

# For most configuration files from conf-available/, which are
# enabled or disabled at a global level, it is possible to
# include a line for only one particular virtual host. For example the
# following line enables the CGI configuration for this host only
# after it has been globally disabled with "a2disconf".
#Include conf-available/serve-cgi-bin.conf
</VirtualHost>

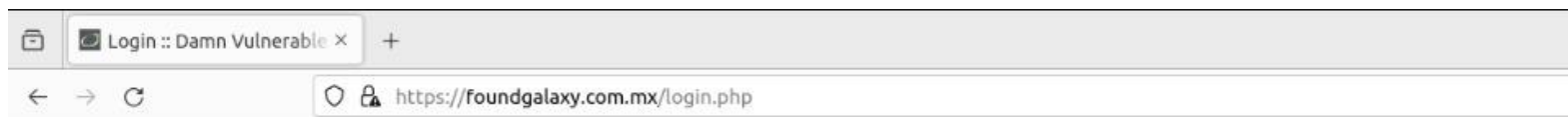
# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
<IfModule mod_ssl.c>
<VirtualHost foundgalaxy.com:443>
ServerName foundgalaxy.com

ServerAdmin webmaster@localhost

DocumentRoot /var/www/html/DVWA

# Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
# error, crit, alert, emerg.
# It is also possible to configure the loglevel for particular
# modules, e.g.
#LogLevel info ssl:warn
```

Configuramos el archivo .conf que previamente copiamos y habilitamos dentro de sites-available para que quede de la siguiente forma y redireccione al usuario de http a https.



Username

Password

Login

## Instalación del certificado SSL autofirmado.

[illegible]

Creamos el par de claves y certificado autofirmados con OpenSSL mediante el siguiente comando: “`sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/apache-selfsigned.key -out /etc/ssl/certs/apache-selfsigned.crt`”

## Configuramos el archivo .conf del VirtualHost para colocar nuestras claves del certificado autofirmado.

## Verificamos el certificado autofirmado.