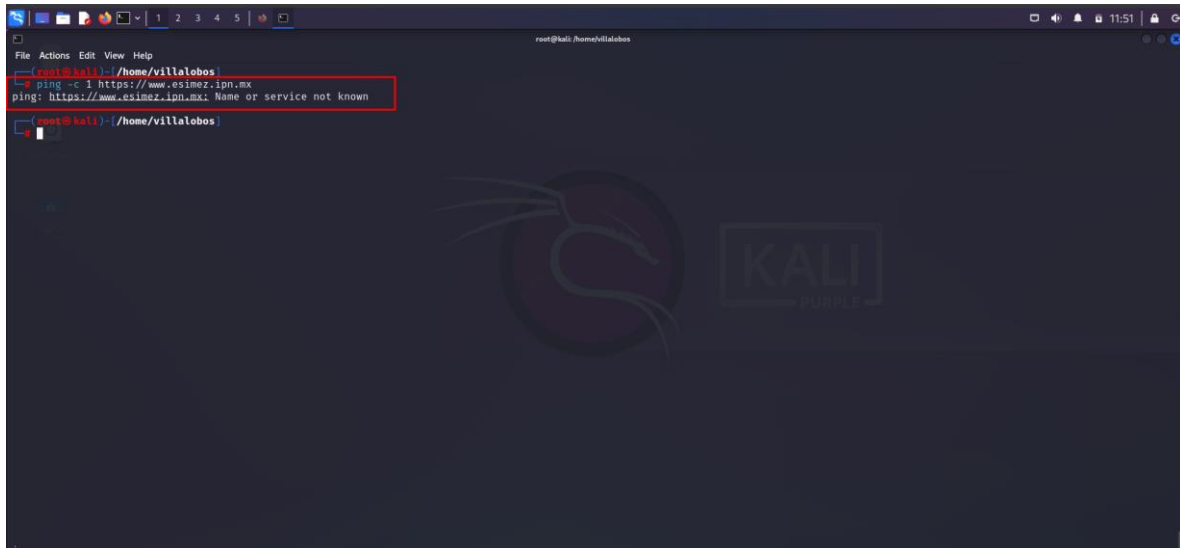


# Reconocimiento

EZIME ZACATENCO

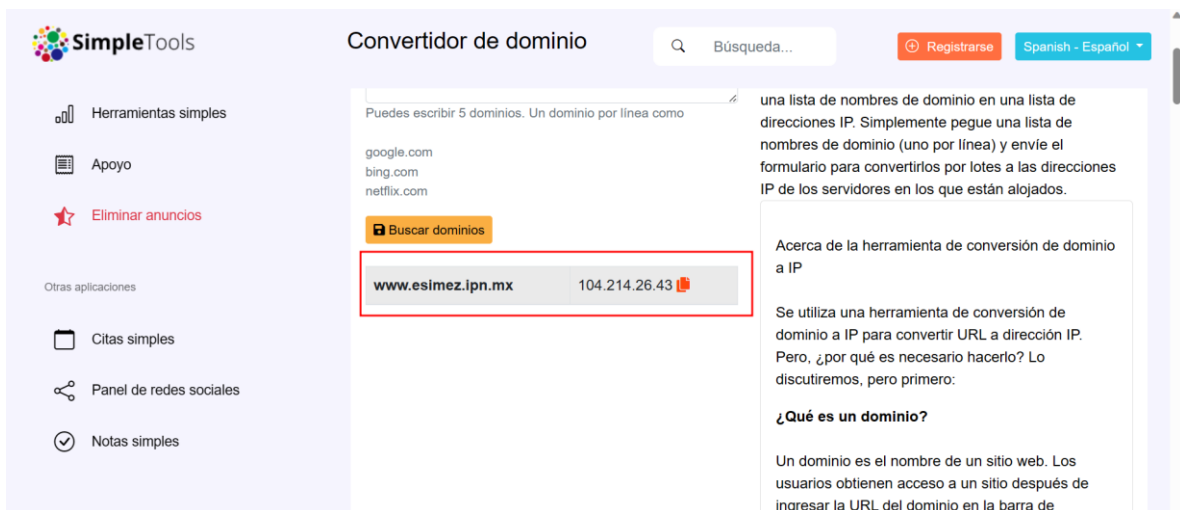
[Portal web de la ESIME Unidad Zacatenco. - ESIMEZ \(ipn.mx\)](https://www.esimez.ipn.mx)

Al principio no logramos hacer ping.



```
root@kali: /home/villalobos
root@kali:~# ping -c 1 https://www.esimez.ipn.mx
ping: https://www.esimez.ipn.mx: Name or service not known
root@kali:~#
```

Buscamos en una web la IP con el dominio que tenemos.



**SimpleTools** Convertidor de dominio

Puedes escribir 5 dominios. Un dominio por línea como

google.com  
bing.com  
netflix.com

**Buscar dominios**

www.esimez.ipn.mx	104.214.26.43
-------------------	---------------


una lista de nombres de dominio en una lista de direcciones IP. Simplemente pegue una lista de nombres de dominio (uno por línea) y envíe el formulario para convertirlos por lotes a las direcciones IP de los servidores en los que están alojados.

Acerca de la herramienta de conversión de dominio a IP

Se utiliza una herramienta de conversión de dominio a IP para convertir URL a dirección IP. Pero, ¿por qué es necesario hacerlo? Lo discutiremos, pero primero:

**¿Qué es un dominio?**

Un dominio es el nombre de un sitio web. Los usuarios obtienen acceso a un sitio después de ingresar la URL del dominio en la barra de



The screenshot shows a Kali Linux terminal window. The title bar at the top indicates the user is root@kali in the directory /home/villalobos. The terminal content shows the user executing a ping command to 104.214.26.43. The output shows a successful ping with 56(84) bytes of data and a TTL of 118. Below the ping output, the user has entered a command to clear the screen (clear), which has not yet been executed as the cursor is still on the same line.

```
root@kali:~/home/villalobos# ping -c 1 104.214.26.43
PING 104.214.26.43 (104.214.26.43) 56(84) bytes of data:
64 bytes from 104.214.26.43: icmp_seq=1 ttl=118 time=179 ms

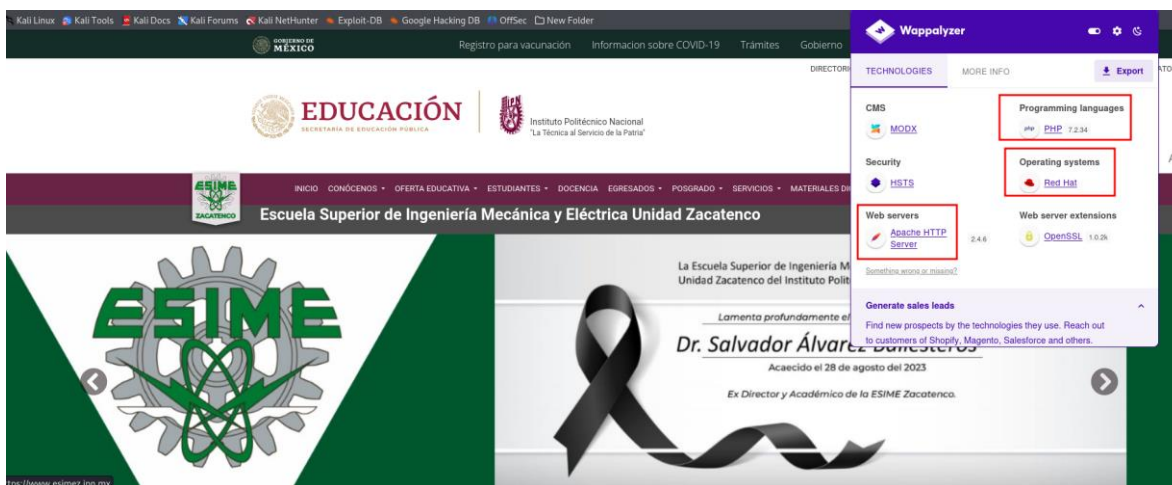
--- 104.214.26.43 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 178.854/178.854/178.854/0.000 ms

root@kali:~/home/villalobos# clear
```



The screenshot shows the top portion of the ESIME Zacateco website. The browser's address bar displays the URL <https://www.esimez.ipn.mx>. The website's header includes the Mexican Government logo and the text "GOBIERNO DE MÉXICO", followed by navigation links: "Registro para vacunación", "Información sobre COVID-19", "Trámites", "Gobierno", and "English". Below this is a secondary navigation bar with links: "DIRECTORIO", "CORREO ELECTRÓNICO", "CALENDARIO", "TRANSPARENCIA", and "PROTECCIÓN DE DATOS". The main header features the "EDUCACIÓN SECRETARÍA DE EDUCACIÓN PÚBLICA" logo on the left and the "IPN Instituto Politécnico Nacional 'La Técnica al Servicio de la Patria'" logo on the right. A dark purple navigation bar contains links: "INICIO", "CONOCÉNDOS", "OFERTA EDUCATIVA", "ESTUDIANTES", "DOCENCIA", "EGRESADOS", "POSGRADO", "SERVICIOS", and "MATERIALES DIGITALES". Below this is a dark grey banner with the text "Escuela Superior de Ingeniería Mecánica y Eléctrica Unidad Zacateco". The bottom section of the banner is green and features the ESIME logo on the left and the text "ETS Septiembre 2023" on the right, with a right-pointing arrow.

Tecnología:



Sistema operativo: Red Hat

Credenciales: No, porque no hay un login.

Activo: Si

Alcance: <https://www.esimez.ipn.mx>



## Mapeo

## Puertos:

```
root@kali: /home/villalobos
File Actions Edit View Help
root@kali ~ - ssh://104.214.26.43
[~] (root@kali) ~ - ssh://104.214.26.43
# nmap -p- 104.214.26.43 --min-rate 5000 -Pn -n -vvv -sS
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-05 12:01 CST
Initiating SYN Stealth Scan at 12:01
Scanning 104.214.26.43 [65535 ports]
Discovered open port 80/tcp on 104.214.26.43
Discovered open port 443/tcp on 104.214.26.43
Increasing send delay for 104.214.26.43 from 0 to 5 due to 11 out of 22 dropped probes since last increase.
Completed SYN Stealth Scan at 12:01, 28.07s elapsed (65535 total ports)
Nmap scan report for 104.214.26.43
Host is up, received user-set (0.28s latency).
Scanned at 2023-09-05 12:01:18 CST for 28s
Not shown: 65532 filtered tcp ports (no-response), 1 filtered tcp ports (admin-prohibited)
PORT      STATE SERVICE REASON
80/tcp    open  http    syn-ack ttl 54
443/tcp   open  https   syn-ack ttl 54
Read data files from: /usr/bin/..share/nmap
Nmap done: 1 IP address (1 host up) scanned in 28.12 seconds
Raw packets sent: 131087 (5.768MB) | Rcvd: 13 (624B)

[~] (root@kali) ~ - ssh://104.214.26.43
```

## Versiones de servicios:

## Para el puerto 80

```
root@kali: /home/villalobos
File Actions Edit View Help
root@kali ~ - ssh://104.214.26.43
[~] (root@kali) ~ - ssh://104.214.26.43
# nmap -p80,443 104.214.26.43 -sVC
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-05 12:04 CST
Nmap scan report for 104.214.26.43
Host is up (0.34s latency).
PORT      STATE SERVICE VERSION
80/tcp    open  http    Microsoft-Azure-Application-Gateway/v2
https-tls? ssl? not found
fingerprint-strings:
  FourOhFourRequest, GetRequest, HTTPOptions:
  HTTP/1.1 404 Not Found
  Server: Microsoft-Azure-Application-Gateway/v2
  Date: Tue, 05 Sep 2023 18:04:12 GMT
  Content-Type: text/html
  Content-Length: 179
  Connection: close
  <html>
  <head><title>404 Not Found</title></head>
  <body>
  <center><h1>404 Not Found</h1></center>
  <hr><center>Microsoft-Azure-Application-Gateway/v2</center>
  </body>
  </html>
RTSPRequest:
  <html>
  <head><title>400 Bad Request</title></head>
  <body>
  <center><h1>400 Bad Request</h1></center>
  <hr><center>Microsoft-Azure-Application-Gateway/v2</center>
  </body>
  </html>
XIIProbe:
  HTTP/1.1 400 Bad Request
  Server: Microsoft-Azure-Application-Gateway/v2
  Date: Tue, 05 Sep 2023 18:04:12 GMT
  Content-Type: text/html
```

## Para el puerto 443

```
root@kali: ~/home/vitalobos
File Actions Edit View Help
| http-server-header: Microsoft-Azure-Application-Gateway/v2
443/tcp open ssl/https Microsoft-Azure-Application-Gateway/v2
| http-server-header: Microsoft-Azure-Application-Gateway/v2
| http-title: 404 Not Found
| ssl-cert: Subject: commonName=ipn.mx
| Subject Alternative Name: DNS:abogadogeneral.ipn.mx, DNS:cda.ipn.mx, DNS:cenac.ipn.mx, DNS:cenlexz.ipn.mx, DNS:cocendi.ipn.mx, DNS:cocnp.ipn.mx, DNS:codigodeconducta.ipn.mx, DNS:cofaa.ipn.mx, DNS:coriyp.ipn.mx, DNS:cultura.ipn.mx, DNS:dae.ipn.mx, DNS:datosabiertos.ipn.mx, DNS:dch.ipn.mx, DNS:dcyc.ipn.mx, DNS:decanato.ipn.mx, DNS:defensoria.ipn.mx, DNS:dems.ipn.mx, DNS:depor-tes.ipn.mx, DNS:des.ipn.mx, DNS:dfle.ipn.mx, DNS:dfi.ipn.mx, DNS:frances.ipn.mx, DNS:genero.ipn.mx, DNS:ingles.ipn.mx, DNS:innovacion.ipn.mx, DNS:investigacion.ipn.mx, DNS:i-
pn.mx, DNS:nanocentro.ipn.mx, DNS:oic.ipn.mx, DNS:poli.ipn.mx, DNS:polivirtual.ipn.mx, DNS:posgrado.ipn.mx, DNS:prestaciones.capitalhumano.ipn.mx, DNS:radio.ipn.mx, DNS:reconstruccion.ipn.mx, DNS:saes.ipn.mx, DNS:seacademica.ipn.mx, DNS:secadministracion.ipn.mx, DNS:sg.ipn.mx, DNS:sip.ipn.mx, DNS:sse.ipn.mx, DNS:stomas.cenlex.ipn.mx, DNS:sustentabilidad.ipn.mx, DNS:tutorias.ipn.mx, DNS:www.abogadogeneral.ipn.mx, DNS:www.cda.ipn.mx, DNS:www.cenac.ipn.mx, DNS:www.cenlexz.ipn.mx, DNS:www.cocendi.ipn.mx, DNS:www.cocnp.ipn.mx, DNS:www.codigodeconducta.ipn.mx, DNS:www.cofaa.ipn.mx, DNS:www.coriyp.ipn.mx, DNS:www.cultura.ipn.mx, DNS:www.dae.ipn.mx, DNS:www.datosabiertos.ipn.mx, DNS:www.dch.ipn.mx, DNS:www.dcyc.ipn.mx, DNS:www.decanato.ipn.mx, DNS:www.def-ensoria.ipn.mx, DNS:www.dems.ipn.mx, DNS:www.deportes.ipn.mx, DNS:www.des.ipn.mx, DNS:www.dfle.ipn.mx, DNS:www.dfi.ipn.mx, DNS:www.dflf.ipn.mx, DNS:www.dsi.ipn.mx, DNS:www.frances.ipn.mx, DNS:www.genero.ipn.mx, DNS:www.ingles.ipn.mx, DNS:www.innovacion.ipn.mx, DNS:www.investigacion.ipn.mx, DNS:www.ipn.mx, DNS:www.nanocentro.ipn.mx, DNS:www.oic.ipn.mx, DNS:www.pol.ipn.mx, DNS:www.polivirtual.ipn.m
x, DNS:www.posgrado.ipn.mx, DNS:www.prestaciones.capitalhumano.ipn.mx, DNS:www.radio.ipn.mx, DNS:www.reconstruccion.ipn.mx, DNS:www.saes.ipn.mx, DNS:www.seacademica.ipn.mx, DNS:www.secadmin-istracion.ipn.mx, DNS:www.sg.ipn.mx, DNS:www.sip.ipn.mx, DNS:www.sse.ipn.mx, DNS:www.stomas.cenlex.ipn.mx, DNS:www.sustentabilidad.ipn.mx, DNS:www.tutorias.ipn.mx
| Not valid after: 2023-10-24T22:56:09
| fingerprint-strings:
  FourOhFourRequest, GetRequest, HTTPOptions:
    HTTP/1.1 404 Not Found
  Server: Microsoft-Azure-Application-Gateway/v2
  Date: Tue, 05 Sep 2023 18:04:18 GMT
  Content-Type: text/html
  Content-Length: 179
  Connection: close
  <html>
  <head><title>404 Not Found</title></head>
  <body>
  <center><h1>404 Not Found</h1></center>
  <hr><center>Microsoft-Azure-Application-Gateway/v2</center>
  </body>
  </html>
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
=====
NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)
SF-Port80-TCP:V=7.94K1=7XD=9/SKTime=64F76D9A&P=x86_64-pc-linux-gnuKr(GetRe
SF:quest,163,"HTTP/1.1:\x20404\x20Not\x20Found\r\nServer:\x20Microsoft-Azu
SF:re-Application-Gateway/v2\r\nDate:\x20Tue,\x2005\x20Sep\x202023\x2018:0
SF:4:12\x20GMT\r\nContent-Type:\x20text/html\r\nContent-Length:\x20179\r\n
=====
```

## Testfire -TLS:

```
root@kali: ~/home/vitalobos/Documents/testssl.sh-3.0.8
File Actions Edit View Help
rDNS (104.214.26.43): --
Service detected: HTTP

Testing protocols via sockets except NPN+ALPN.
SSLV2      not offered (OK)
SSLV3      not offered (OK)
TLS 1      offered (deprecated)
TLS 1.1    offered (deprecated)
TLS 1.2    offered (OK)
TLS 1.3    not offered and downgraded to a weaker protocol
NPN/SPDY   http/1.1 (advertised)
ALPN/HTTP2 http/1.1 (offered)

Testing cipher categories.
NULL ciphers (no encryption)      not offered (OK)
Anonymous NULL ciphers (no authentication) not offered (OK)
Export ciphers (w/o ADH+NULL)     not offered (OK)
LOW: 64 bit + DES, RC[2,4] (w/o export) not offered (OK)
Triple DES Ciphers / IDEA        not offered
Obsolete CBC ciphers (AES, ARIA etc.) offered
Strong encryption (AEAD ciphers)  offered (OK)

Testing robust (perfect) forward secrecy, (PFS -- omitting Null Authentication/Encryption, 3DES, RC4)
PFS is offered (OK)
Elliptic curves offered: prime256v1
ECDHE-ECDSA-AES256-GCM-SHA384, ECDHE-ECDSA-AES256-SHA384, ECDHE-ECDSA-AES256-SHA, ECDHE-ECDSA-AES128-GCM-SHA256, ECDHE-ECDSA-AES128-SHA256, ECDHE-ECDSA-AES128-SHA

Testing server preferences.
Has server cipher order? yes (OK)
Negotiated protocol     TLSv1.2
Negotiated cipher        ECDHE-ECDSA-AES256-GCM-SHA384, 256 bit ECDH (P-256)
Cipher order
```