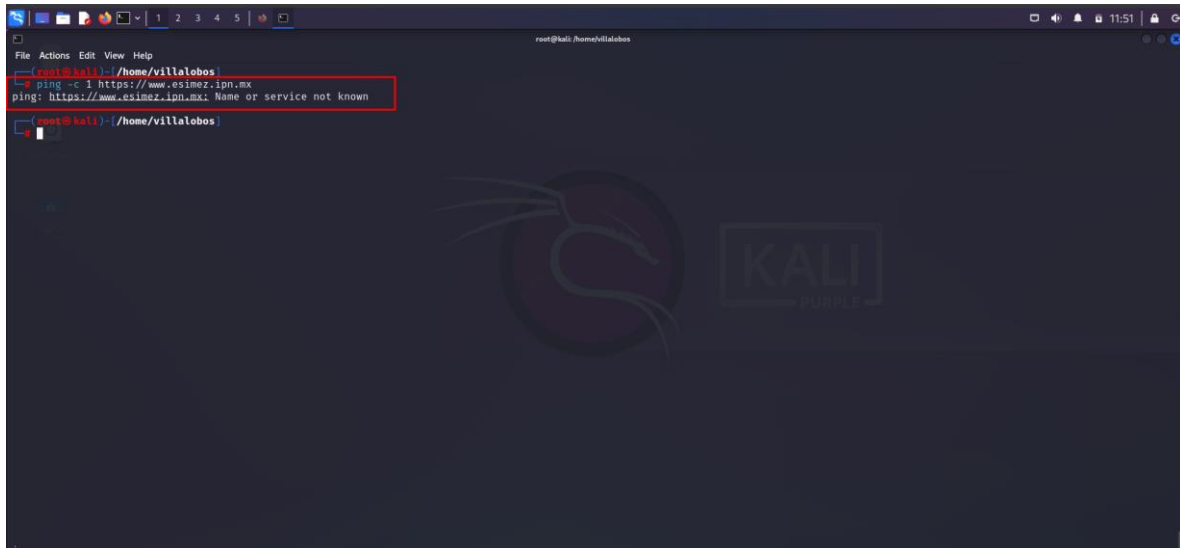


Reconocimiento

EZIME ZACATENCO

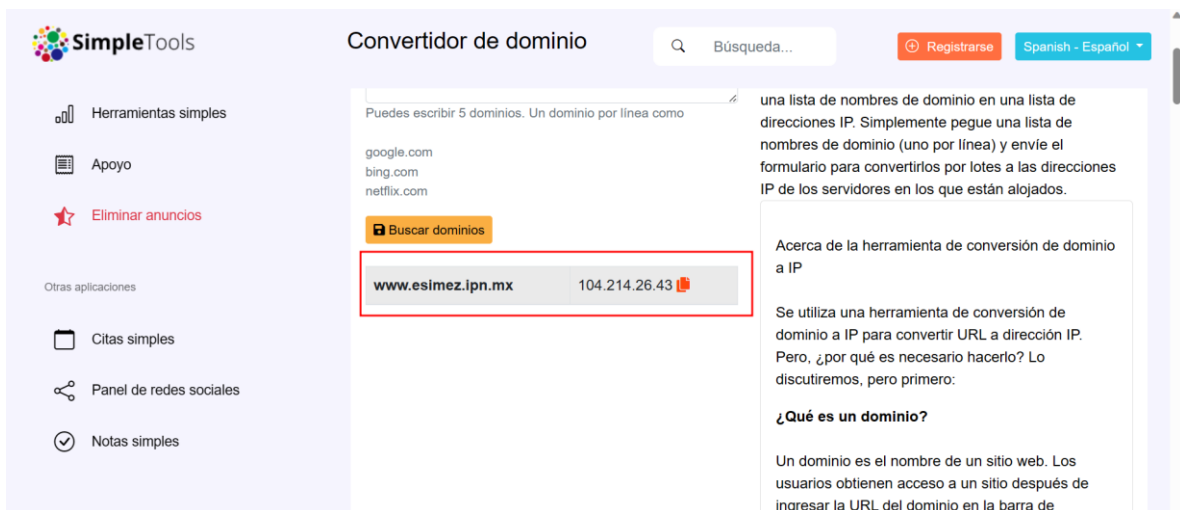
[Portal web de la ESIME Unidad Zacatenco. - ESIMEZ \(ipn.mx\)](https://www.esimez.ipn.mx)

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.



The screenshot shows the SimpleTools website with the 'Convertidor de dominio' (Domain Converter) tool. The tool has a search bar with the text 'Búsqueda...' and a 'Registrarse' button. Below the search bar, there is a list of domains: 'google.com', 'bing.com', and 'netflix.com'. A red box highlights the 'Buscar dominios' button. Below the button, a table shows the conversion of 'www.esimez.ipn.mx' to the IP address '104.214.26.43'. The table has two columns: the domain and the IP address. The domain 'www.esimez.ipn.mx' is highlighted with a red box. The IP address '104.214.26.43' is also highlighted with a red box. To the right of the table, there is a text box explaining the tool's purpose: '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.' Below this, there is a section titled 'Acerca de la herramienta de conversión de dominio a IP' which explains that the tool is used to convert domain names to IP addresses. It also includes a section titled '¿Qué es un dominio?' which defines a domain as the name of a website.

dominio	IP
www.esimez.ipn.mx	104.214.26.43

Sistema operativo: Windows, TTL = 128



Tecnología:



Credenciales: No, porque no hay un login.

Activo: Si

Alcance:



Mapeo

Puertos:

```
root@kali:~/home/villalobos
[~] (root@kali) ~/home/villalobos
# 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) ~/home/villalobos
```

Versiones de servicios:

Para el puerto 80

```
root@kali:~/home/villalobos
[~] (root@kali) ~/home/villalobos
# 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
_ftp_     _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/villalobos
File Actions Edit View Help
https://10.10.10.10:443/
[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:cenlex.ipn.mx, DNS:cocendi.ipn.mx, DNS:ccocnp.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:deportes.ipn.mx, DNS:des.ipn.mx, DNS:dfle.ipn.mx, DNS:drf.ipn.mx, DNS:dsi.ipn.mx, DNS:frances.ipn.mx, DNS:genero.ipn.mx, DNS:ingles.ipn.mx, DNS:innovacion.ipn.mx, DNS:investigacion.ipn.mx, DNS:lab.ipn.mx, DNS:nanocentro.ipn.mx, DNS:oic.ipn.mx, DNS:poi.ipn.mx, DNS:polivirtual.ipn.mx, DNS:posgrado.ipn.mx, DNS:prestaciones.capitalhumano.ipn.mx, DNS:radio.ipn.mx, DNS:reconstruccion.ipn.mx, DNS:sae.ipn.mx, DNS:seacademica.ipn.mx, DNS:seadministracion.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.cenlex.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.defensoria.ipn.mx, DNS:www.dems.ipn.mx, DNS:www.deportes.ipn.mx, DNS:www.des.ipn.mx, DNS:www.dfle.ipn.mx, DNS:www.drf.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.poi.ipn.mx, DNS:www.polivirtual.ipn.mx, DNS:www.posgrado.ipn.mx, DNS:www.prestaciones.capitalhumano.ipn.mx, DNS:www.radio.ipn.mx, DNS:www.reconstruccion.ipn.mx, DNS:www.sae.ipn.mx, DNS:www.seacademica.ipn.mx, DNS:www.seadministracion.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 before: 2023-07-26T22:56:10
Not valid after: 2023-10-24T22:56:09
fingerprint-strings:
  FourDHFourRequest, 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=7.9&X=7&D=9/S&T=64F7609ASP&X=86.64-pc-linux-gnu&r(GetRe
SF-request,153,1,HTTP/1.1\r\n\r\n404\r\n\r\nNot Found\r\n\r\nServer: Microsoft-Azu
SF:re-Application-Gateway/v2\r\n\r\nDate: \r\n\r\nTue, \r\n\r\n2005\r\n\r\n20Sep\r\n\r\n202023\r\n\r\n2018:0
SF:4:12\r\n\r\n20GMT\r\n\r\nContent-Type: \r\n\r\n20text/html\r\n\r\nContent-Length: \r\n\r\n20179\r\n\r\n
```

Testfire-TLS:

```
root@kali: ~/home/villalobos/Documents/testssl.sh-3.0.8
File Actions Edit View Help
rDNS (104.214.26.43): --
Service detected: HTTP
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
DHE is offered (OK)
ECDSA is offered (OK)
Elliptic curves offered: prime256v1
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
```