**OSCAR DAVID MESA CALDERON**

# PUNTO A

Explicar la funcionalidad de 5 tipos de scripts.

La función, los parámetros y requisitos.

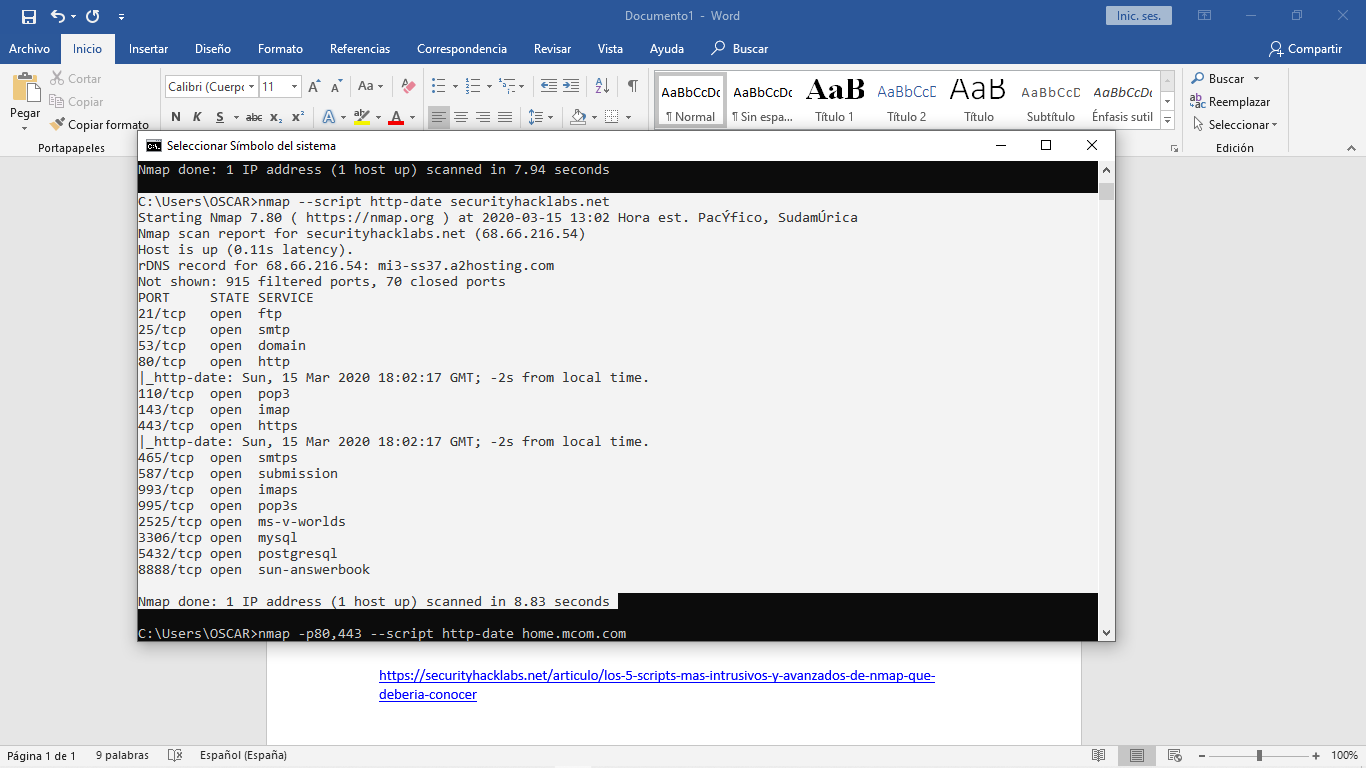
Analizar 5 sitios web.

## **SCRIPT http-date**

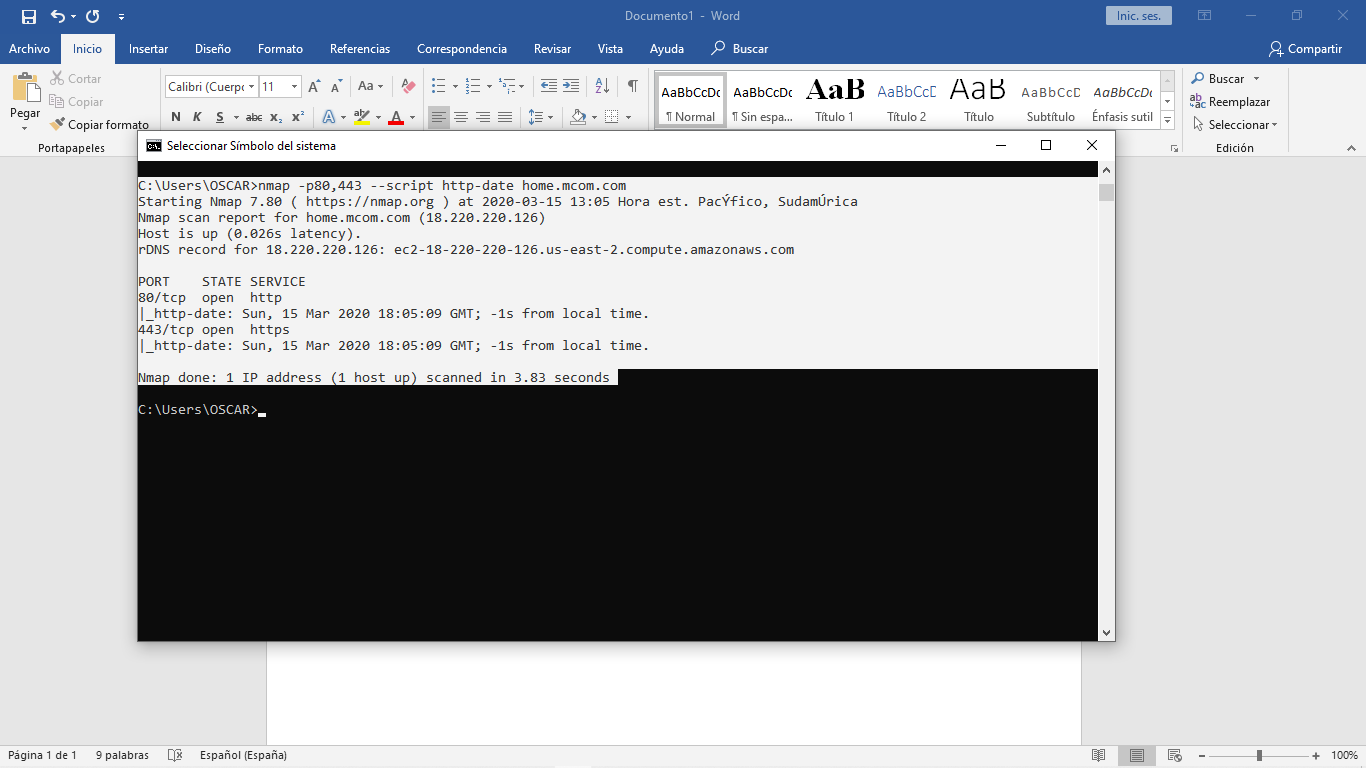
El script consiste en obtener la fecha se servicios http. Lo que genera como salida, cuanto difiera la fecha de la fecha de la hora local.

Donde la hora local es la hora en que se enviar la solicitud http.

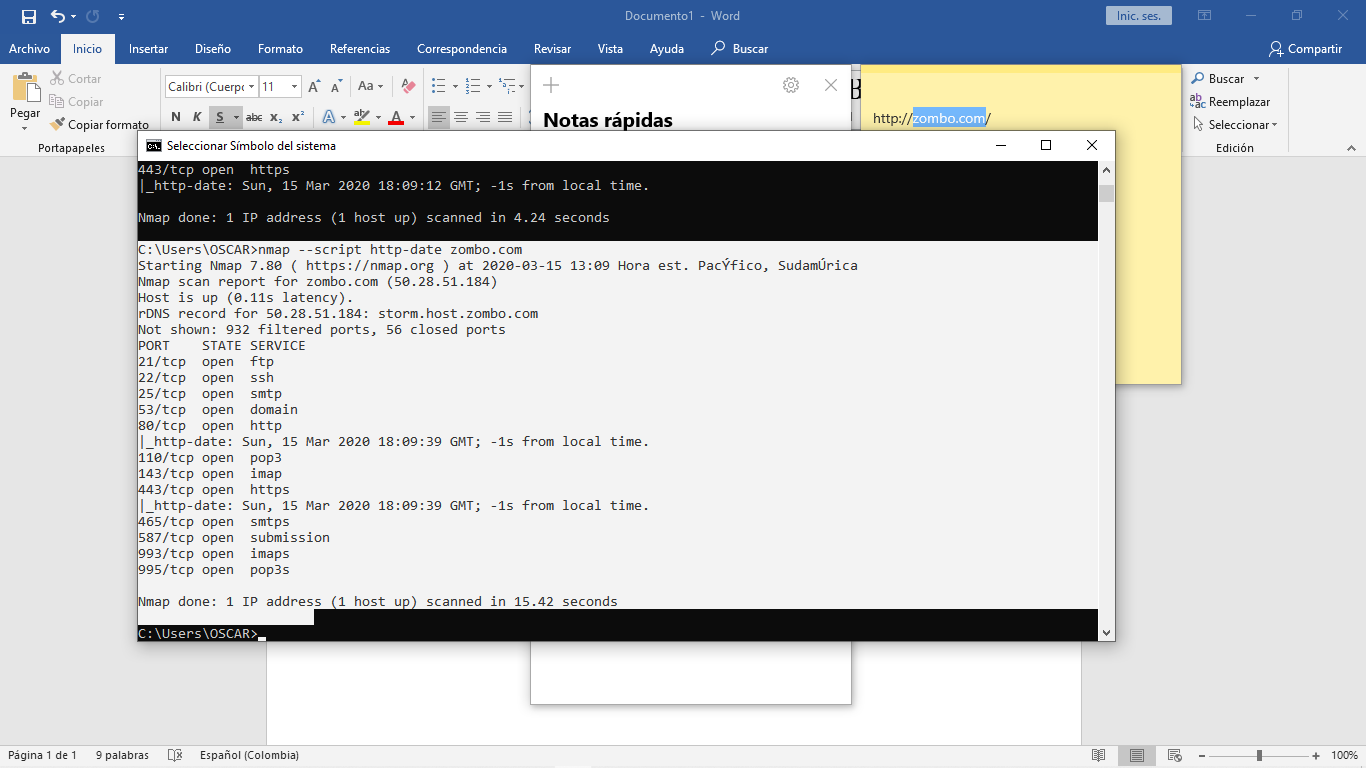
Posibles argumentos para especializar el script: http.host, http.max-body-size, http.max-cache-size, http.max-pipeline, http.pipeline, http.truncated-ok, http.useragent.



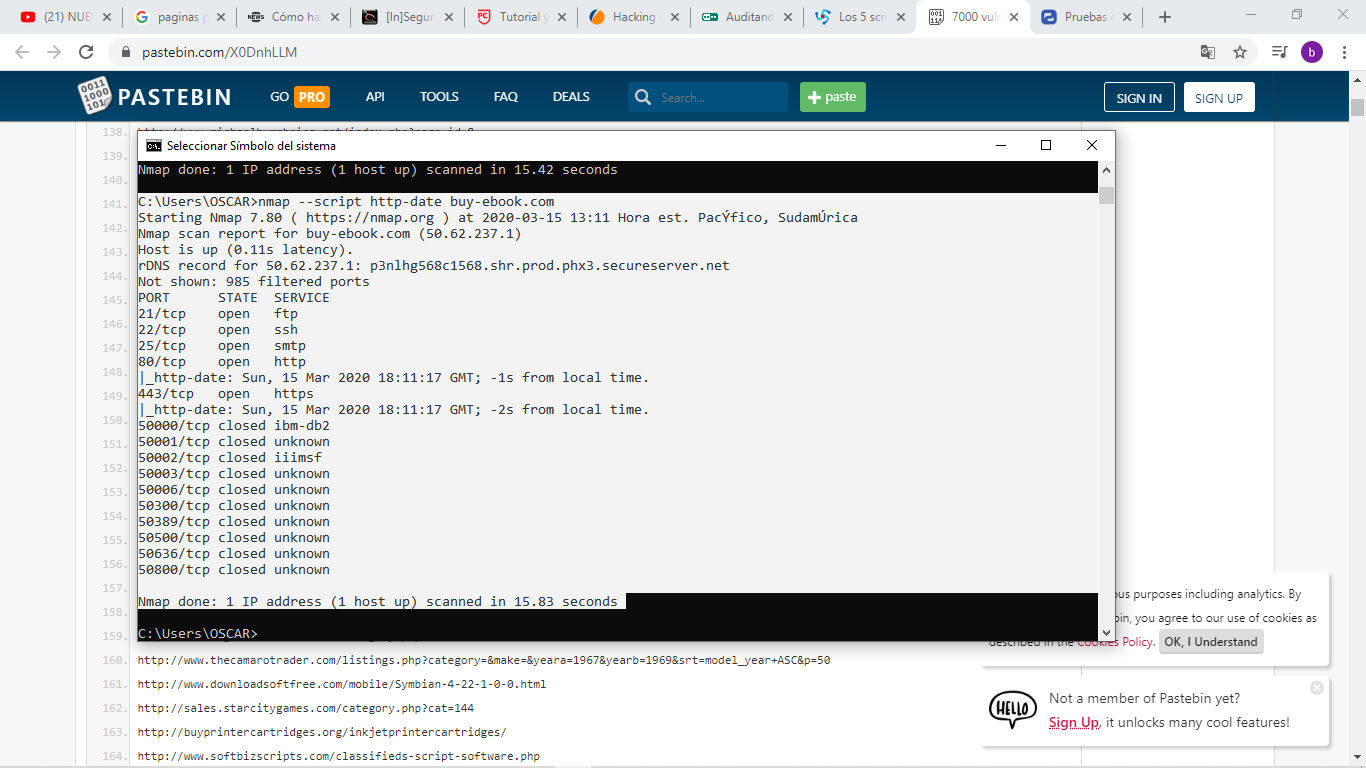
En la página Securityhacklabs, devuelve como respuesta dos solicitudes http en el puerto 80 y 443 con protocolo tcp. Ambos están abiertos y corresponden a servicios http y https. Con un tiempo de respuesta de 2 segundos.



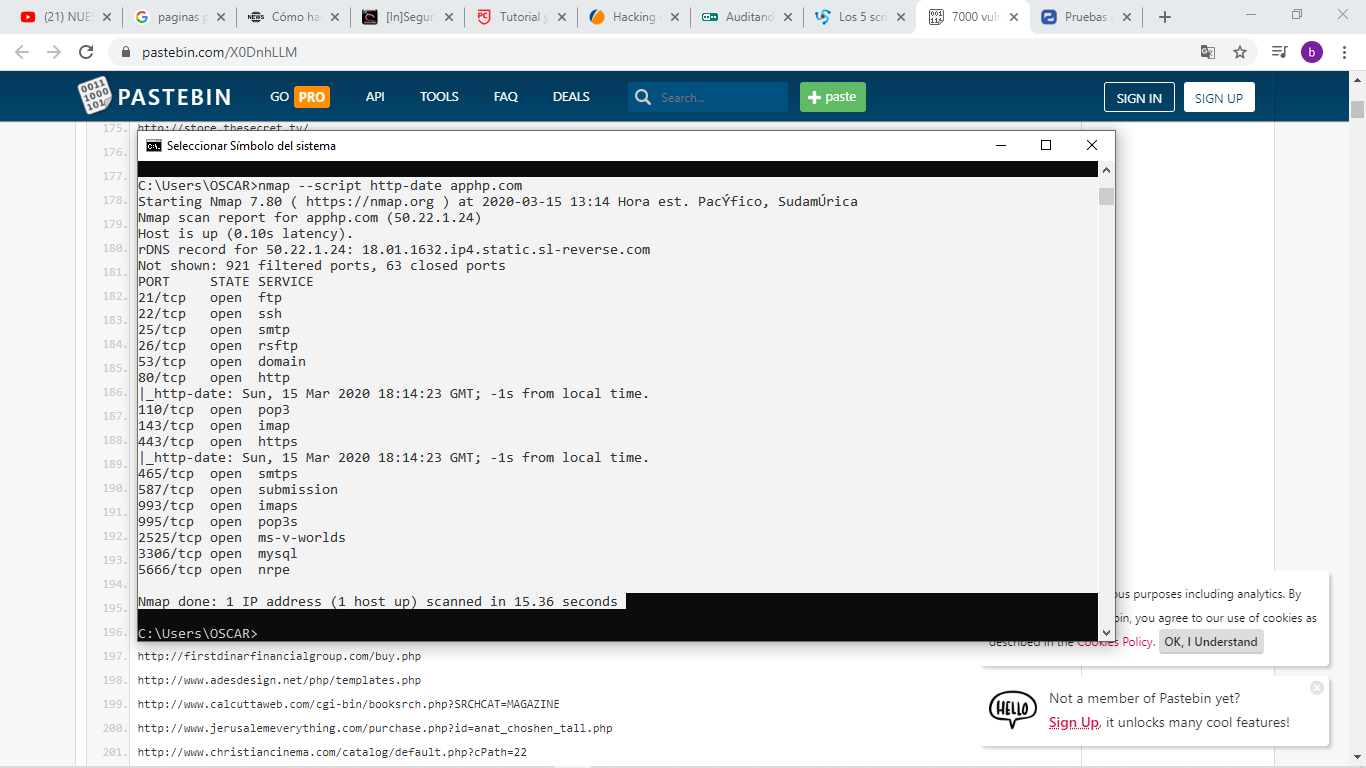
En la página home.mcom.com, devuelve como respuesta dos solicitudes http en el puerto 80 y 443 con protocolo tcp. Ambos están abiertos y corresponden a servicios http y https. Con un tiempo de respuesta de 1 segundos.



En la página zombo.com, devuelve como respuesta dos solicitudes http en el puerto 80 y 443 con protocolo tcp. Ambos están abiertos y corresponden a servicios http y https. Con un tiempo de respuesta de 1 segundos.



En la página buy-ebook.com, devuelve como respuesta dos solicitudes http en el puerto 80 y 443 con protocolo tcp. Ambos están abiertos y corresponden a servicios http y https. Con un tiempo de respuesta de 1 segundos y 2 segundos.

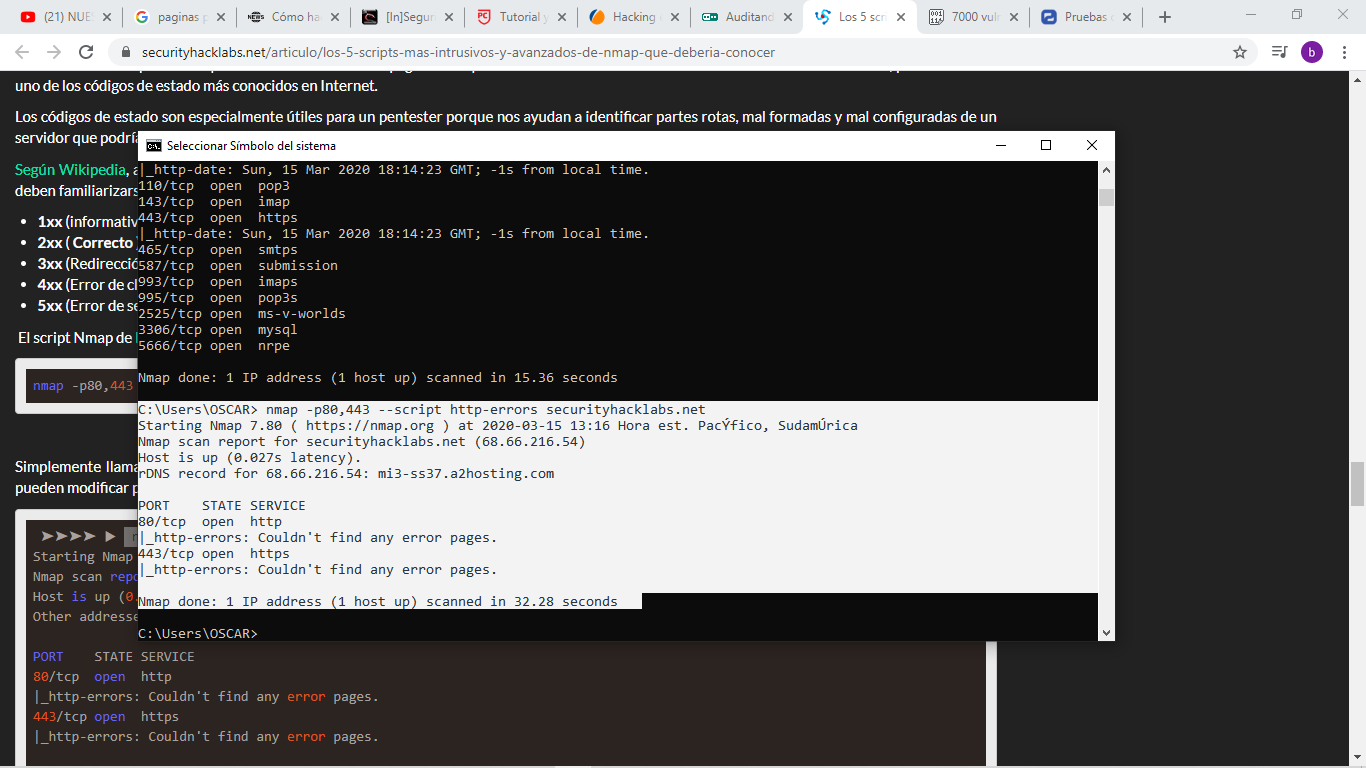


En la página apphp.com, devuelve como respuesta dos solicitudes http en el puerto 80 y 443 con protocolo tcp. Ambos están abiertos y corresponden a servicios http y https. Con un tiempo de respuesta de 1 segundos.

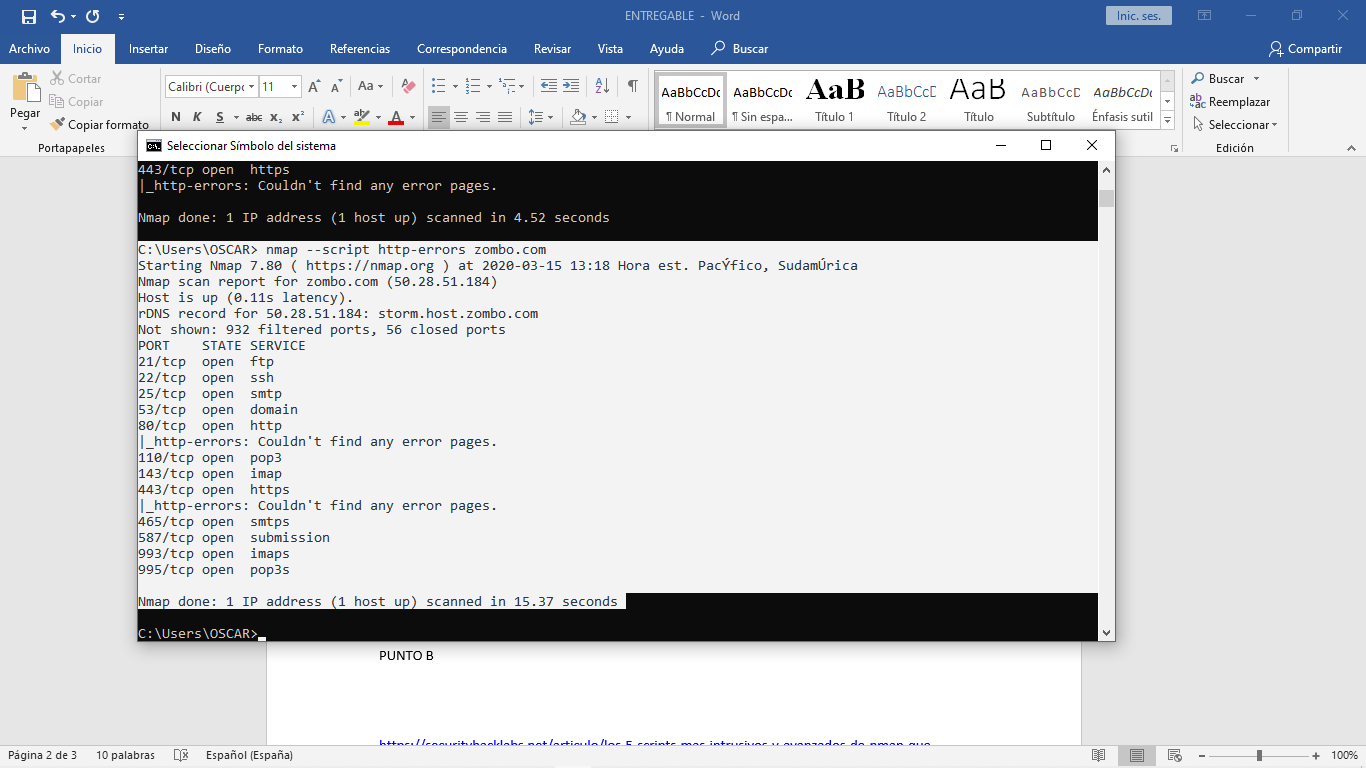
## **SCRIPT http-errors**

El script consiste en obtener el rastreo de la pagina web y los posibles errores en la página de tipo http igual o superior a 400. Su comportamiento es similar al de un spider que por defecto indexa 40 páginas. Si desea aumentar el numero de paginas con el valor de maxpagecount.

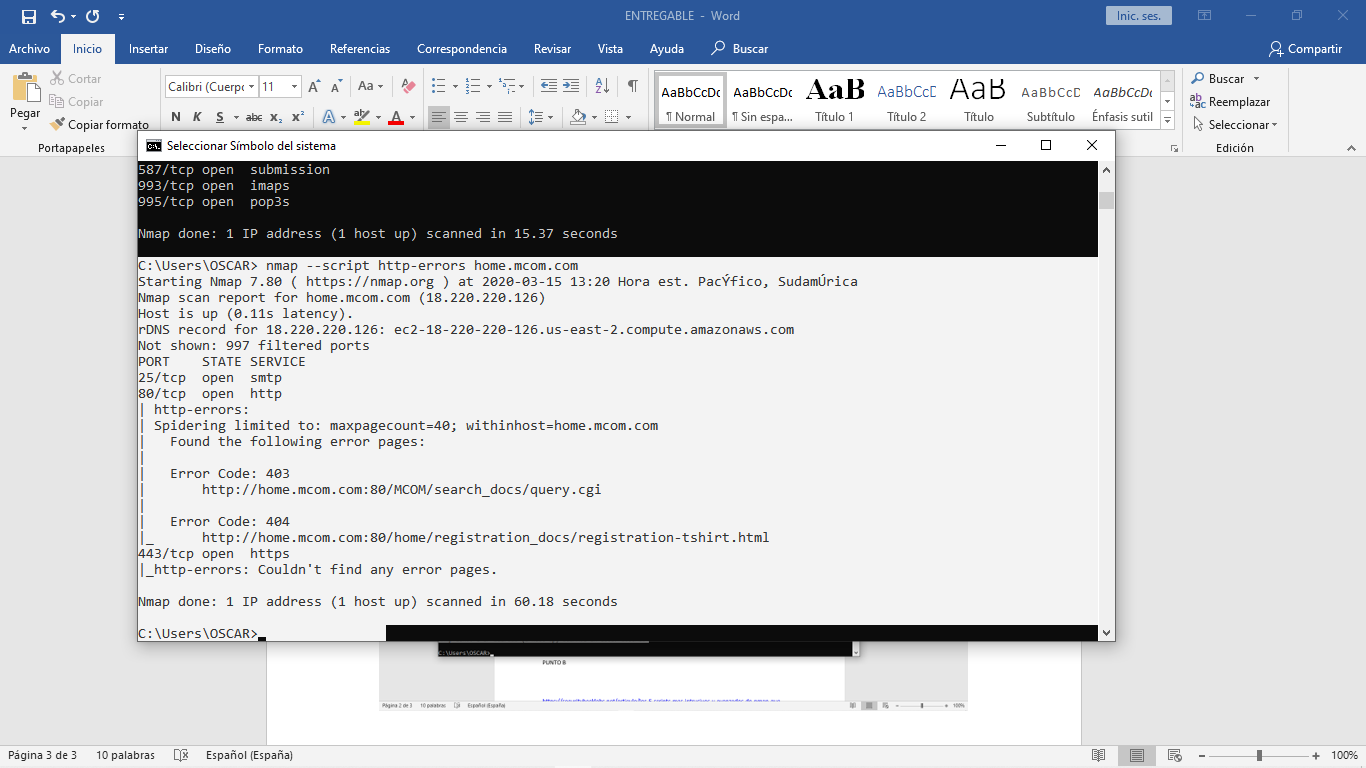
Posibles argumentos para especializar el script: slaxml.debug, httpspider.doscraping, httpspider.maxdepth, httpspider.maxpagecount, httpspider.noblacklist, httpspider.url, httpspider.useheadfornonwebfiles, httpspider.withindomain, httpspider.withinhost, http.host, http.max-body-size, http.max-cache-size, http.max-pipeline, http.pipeline, http.truncated-ok, http.useragent, smbdomain, smbhash, smbnoguest, smbpassword, smbtype, smbusername, http-errors.errcodes.

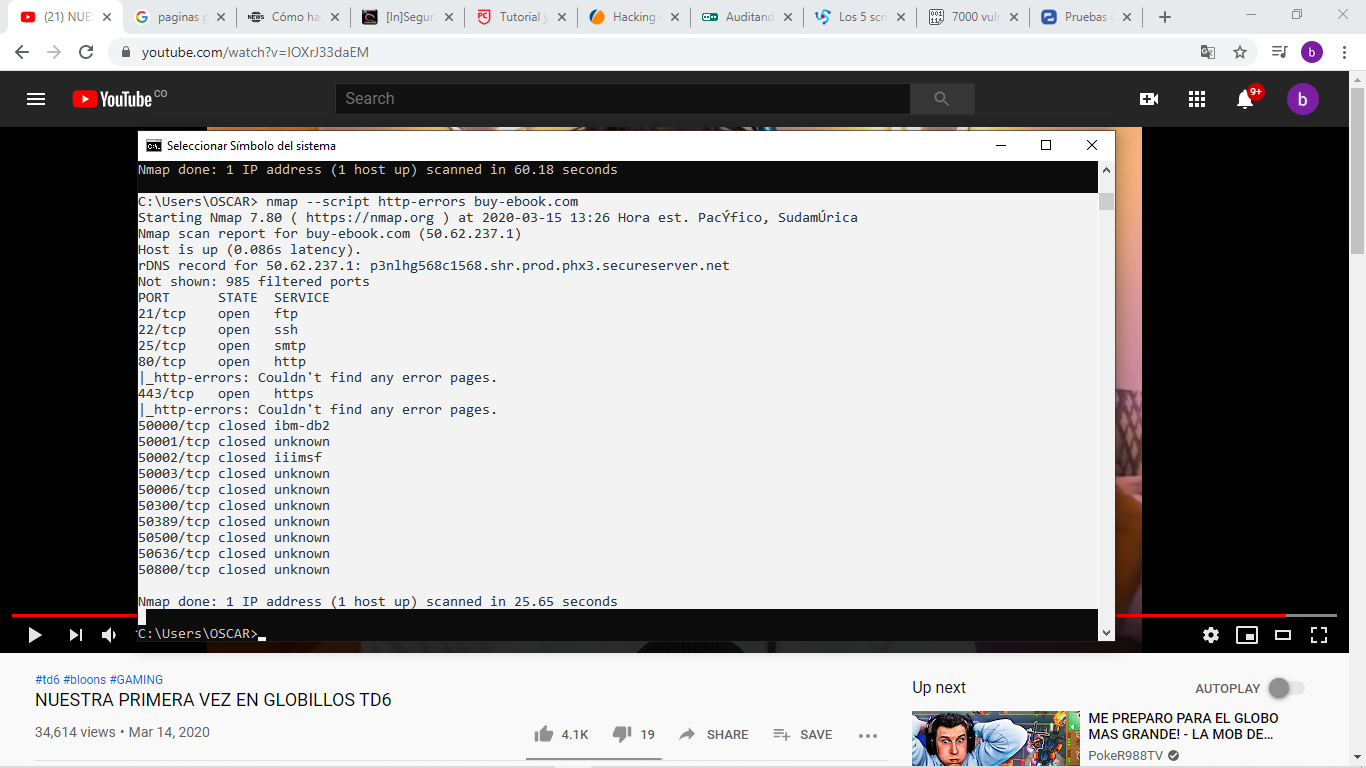


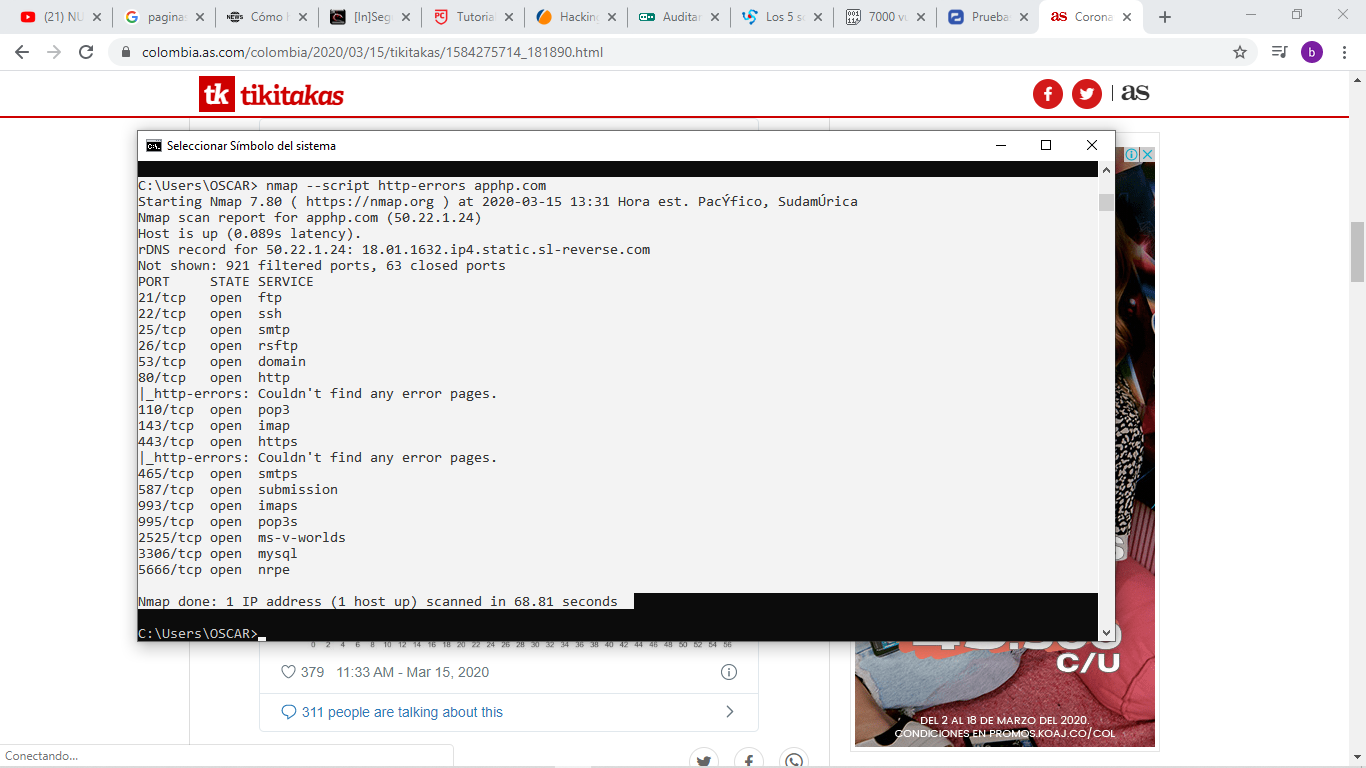
En la página Securityhacklabs, devuelve como respuesta sin ningún error encontrado en los puertos 80 y 443.



En la página Zombo.com, devuelve como respuesta sin ningún error encontrado en los puertos 80 y 443.



En la página home.mcom.com, devuelve como respuesta errores 403 y 404 en el puerto 80 y sin ningún error en el puerto 443. 

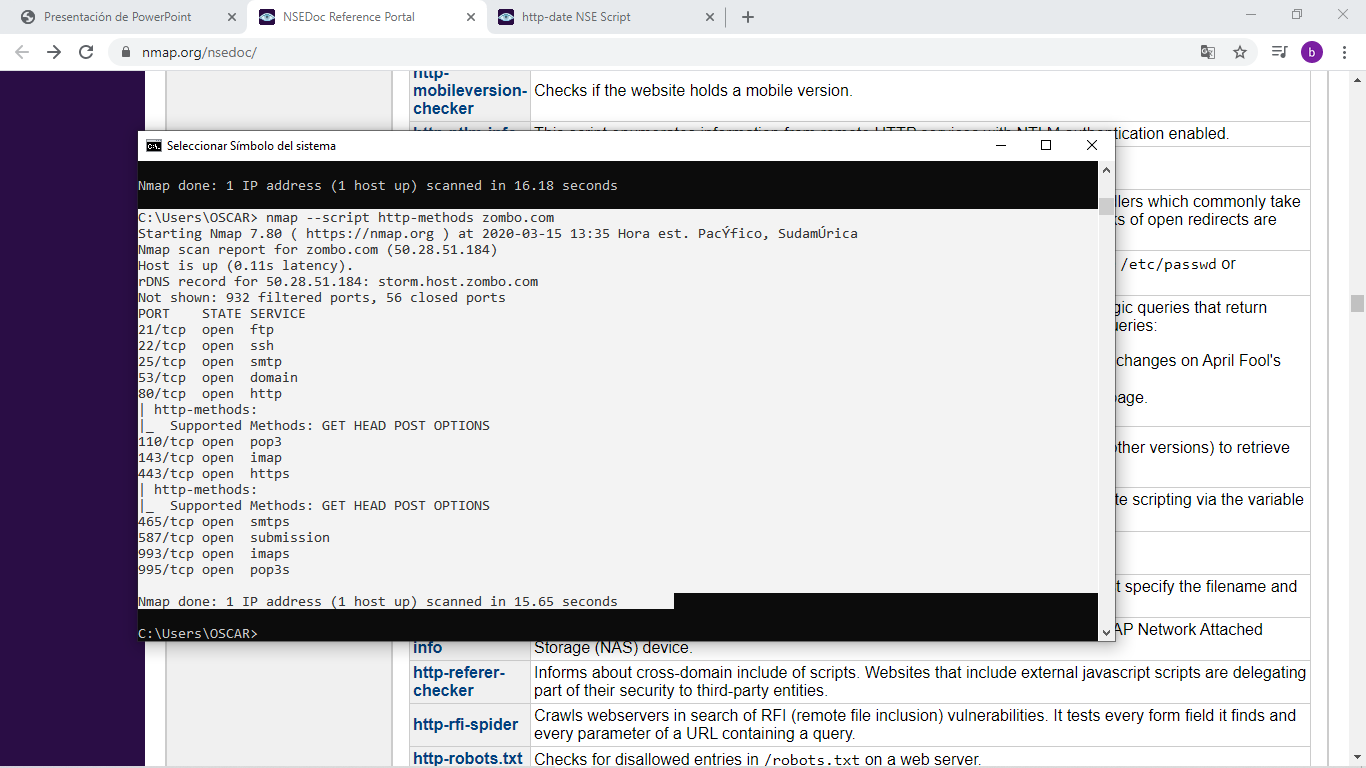
En la página buy-ebook.com, devuelve como respuesta sin ningún error encontrado en los puertos 80 y 443. 

En la página apphp.com, devuelve como respuesta sin ningún error encontrado en los puertos 80 y 443.

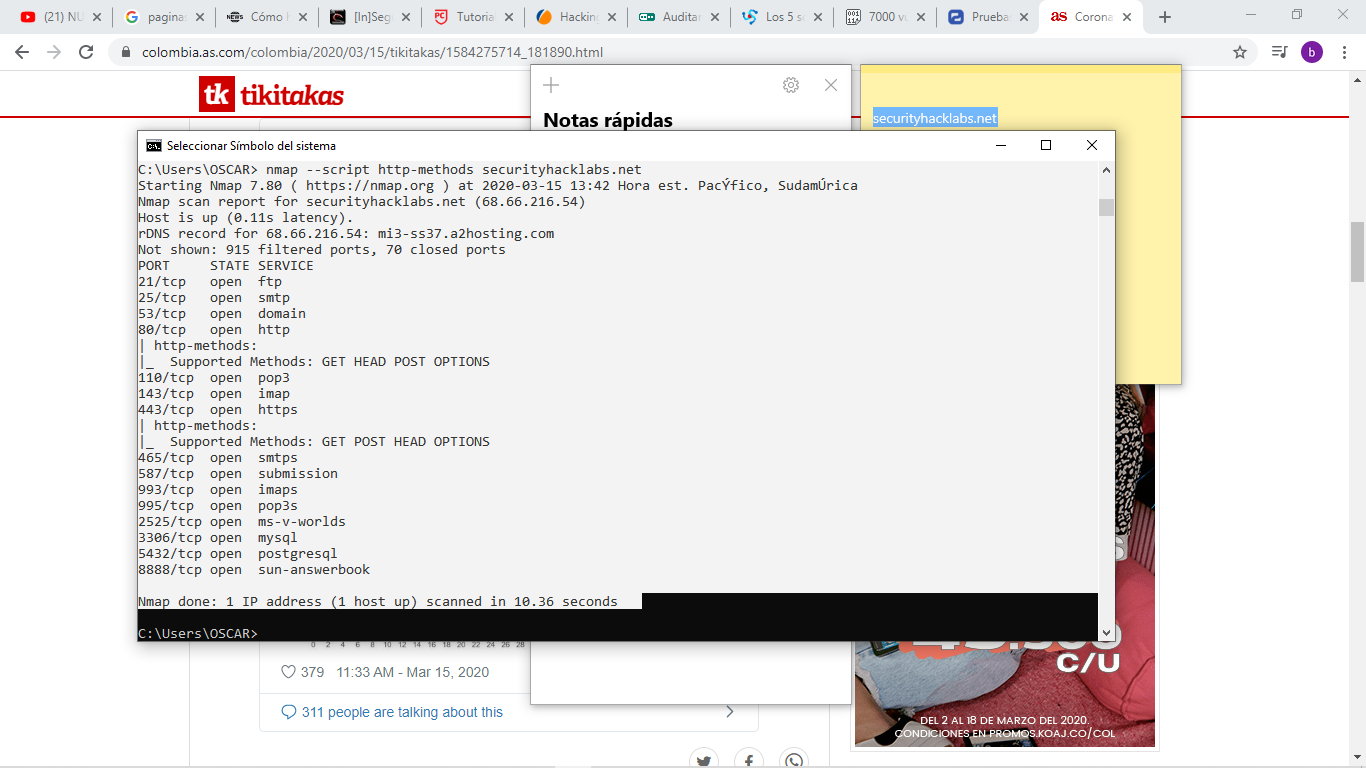
## **SCRIP http—methods**

El script consiste en obtener los métodos del servidor http. Posteriormente enumera métodos potencialmente peligrosos. Comprobando las salidas (respuestas en código).

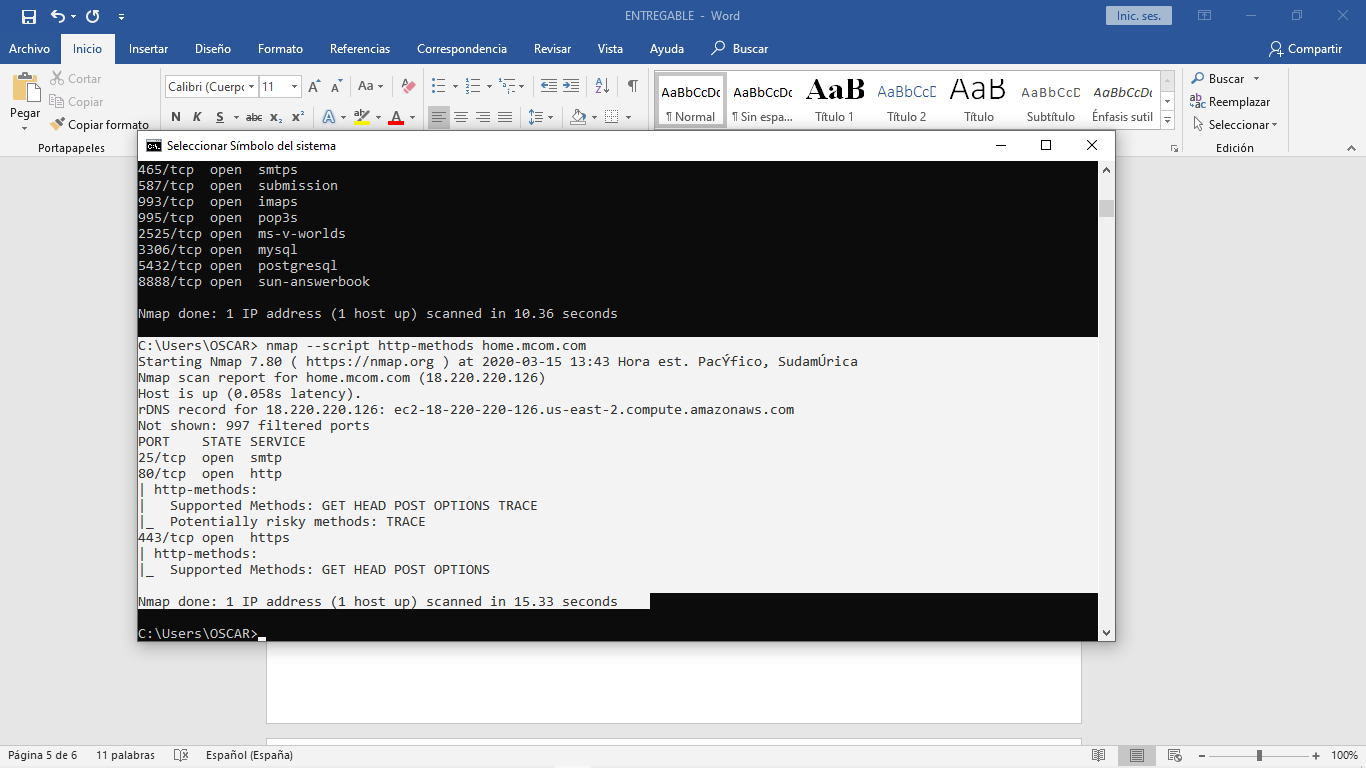
Posibles argumentos para especializar el script: http-method.url-path, http-method.test-all, http-method.retest, slaxml.debug, http.host, http.max-body-size, http.max-cache-size, http.max-pipeline, http.pipeline, http.truncated-ok, http.useragent, smbdomain, smbhash, smbnoguest, smbpassword, smbtype, smbusername



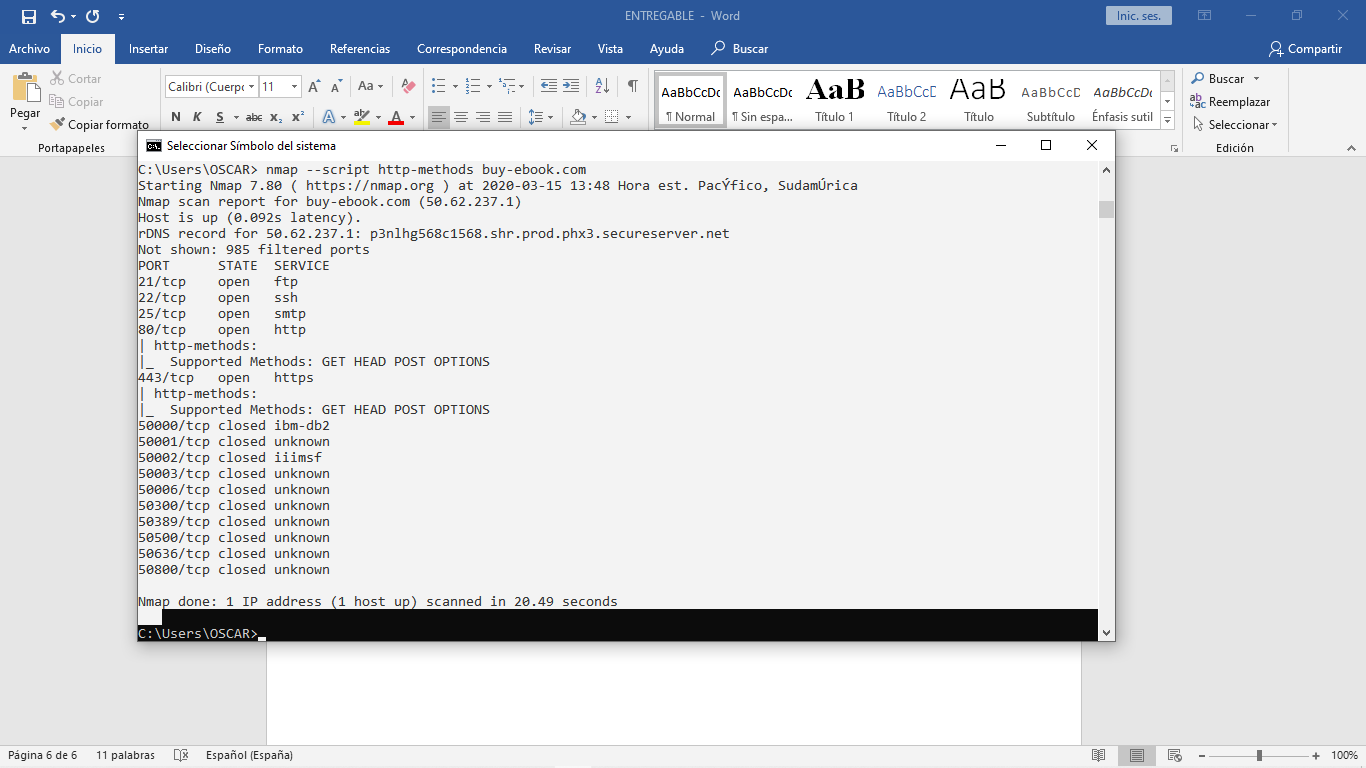
En la página ZOMBO.com, devuelve como respuesta los métodos que recibe los puertos 80 y 443. sin ningún error encontrado.



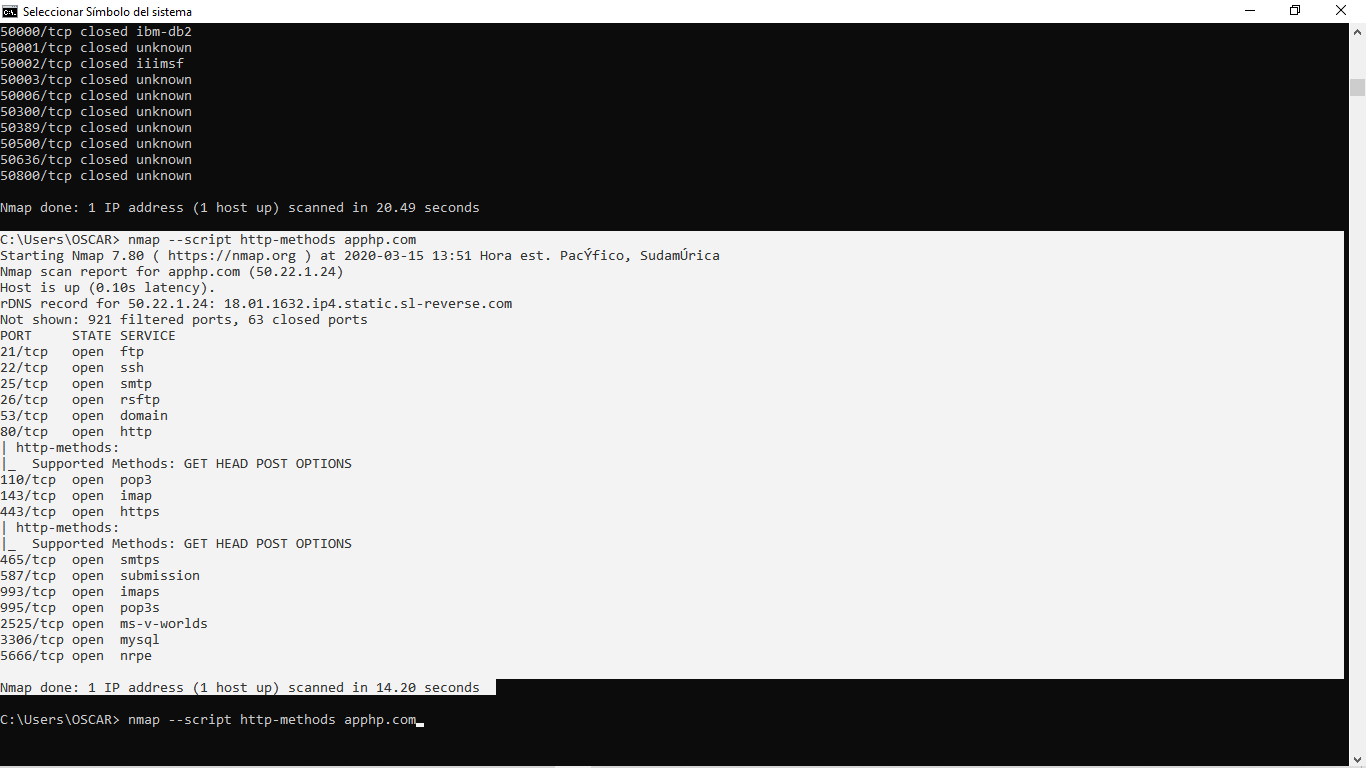
En la página Securityhacklabs, devuelve como respuesta los métodos que recibe los puertos 80 y 443. sin ningún error encontrado.



En la página home.mcom.com, devuelve como respuesta los métodos que recibe los puertos 80 y 443. Encuentra errores en el método TRACE en el puerto 80.



En la página buy-ebook.com, devuelve como respuesta los métodos que recibe los puertos 80 y 443. sin ningún error encontrado.

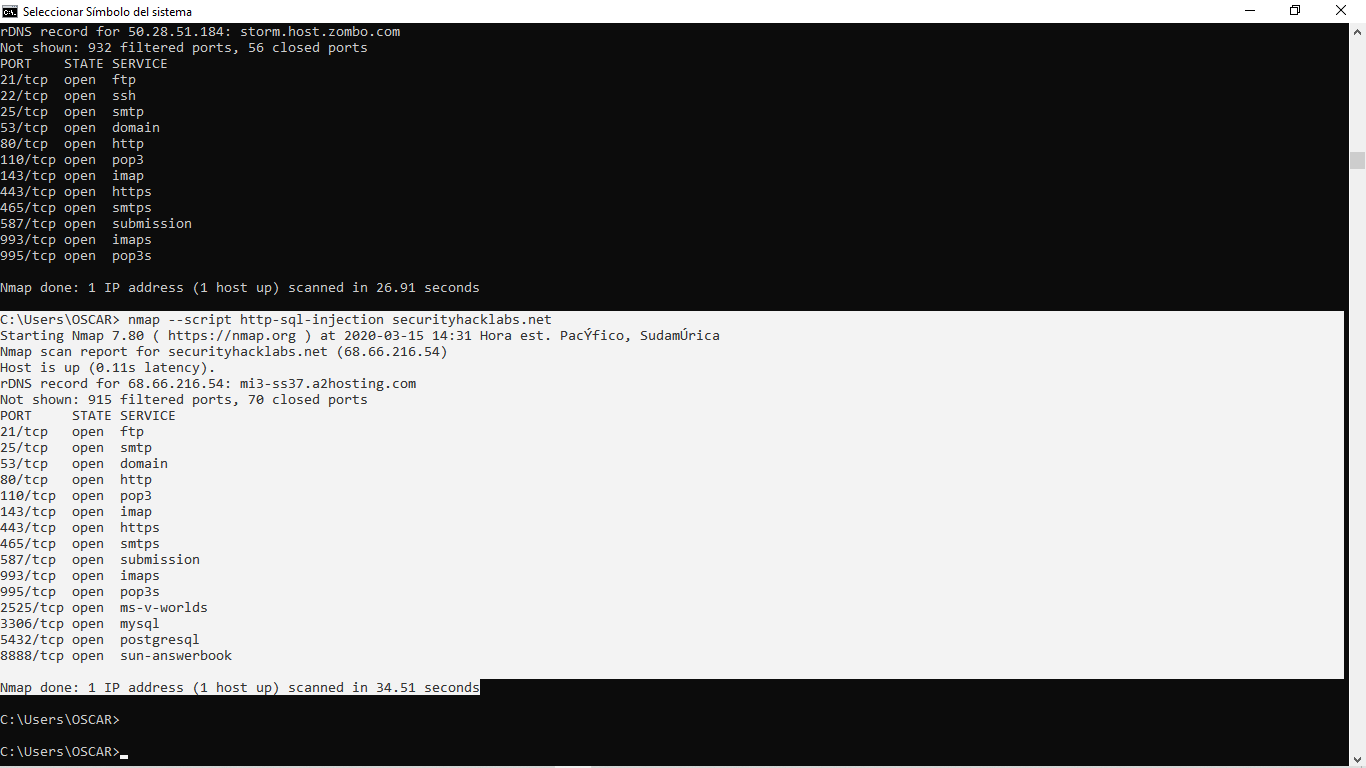


En la página apphp.com, devuelve como respuesta los métodos que recibe los puertos 80 y 443. sin ningún error encontrado

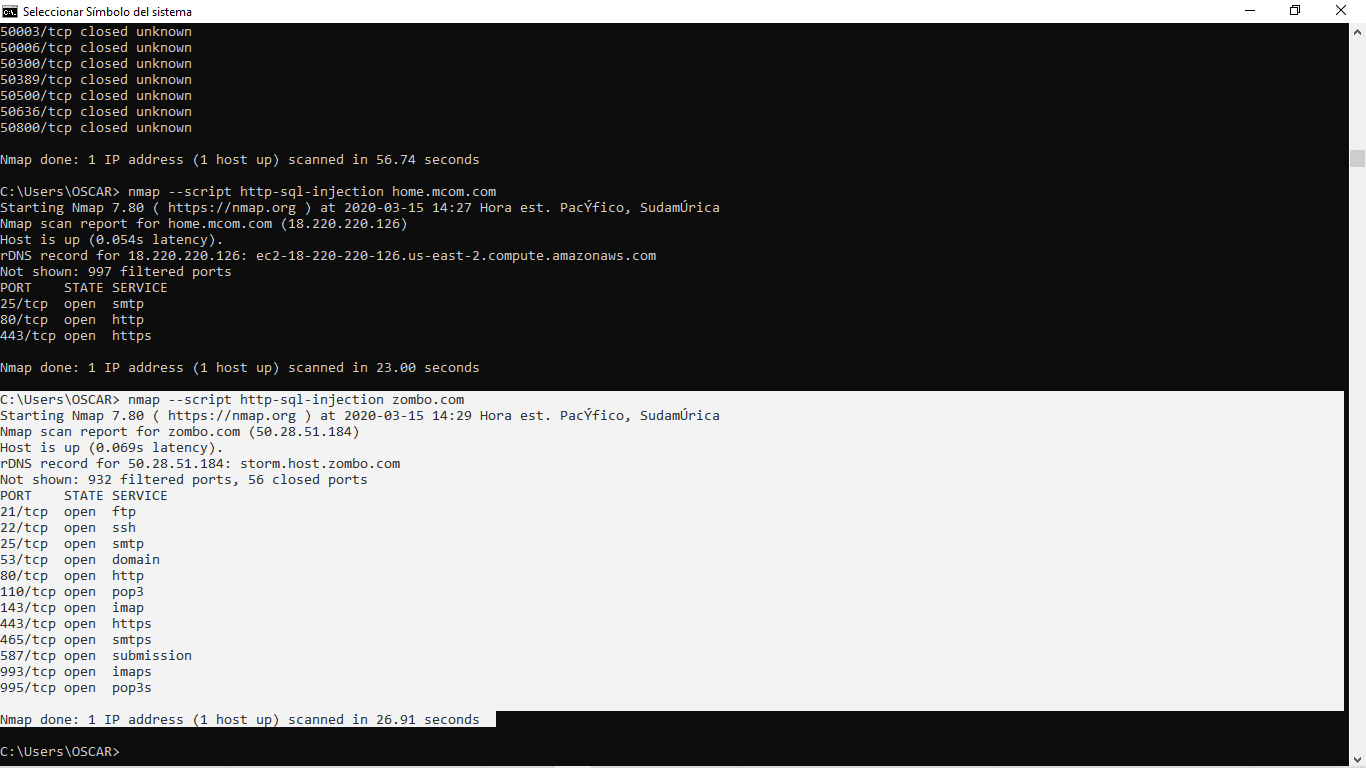
## **Scrip http-sql-injection**

El script consiste en un spider a los servidores http de una url en busca a consultas vulnerables a inyección de sql. Generalmente campos en formularios terminan siendo vulnerables.

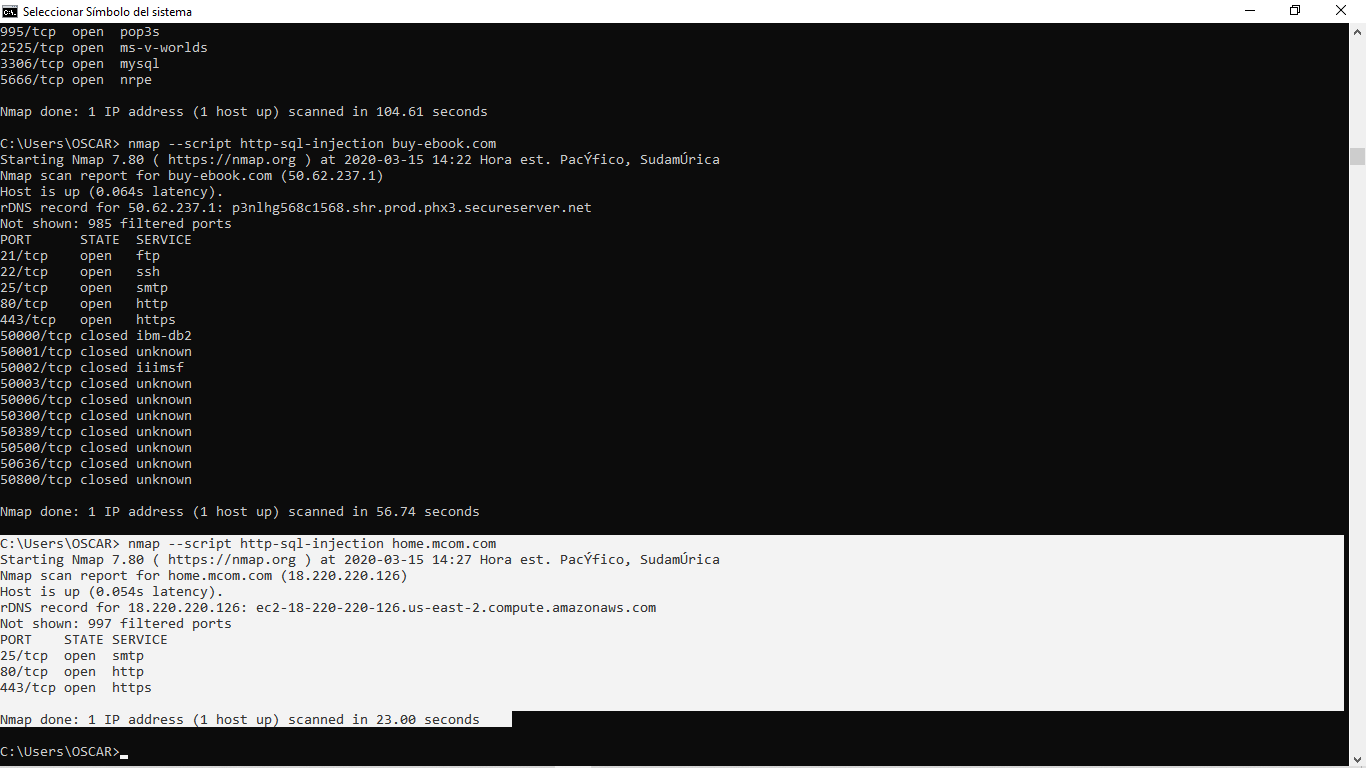
Posibles argumentos para especializar el script: http-sql-injection.withinhost, http-sql-injection.errorstrings, http-sql-injection.withindomain, http-sql-injection.url, http-sql-injection.maxpagecount, slaxml.debug, httpspider.doscraping, httpspider.maxdepth, httpspider.maxpagecount, httpspider.noblacklist, httpspider.url, httpspider.useheadfornonwebfiles, httpspider.withindomain, httpspider.withinhost, smbdomain, smbhash, smbnoguest, smbpassword, smbtype, smbusername, http.host, http.max-body-size, http.max-cache-size, http.max-pipeline, http.pipeline, http.truncated-ok, http.useragent



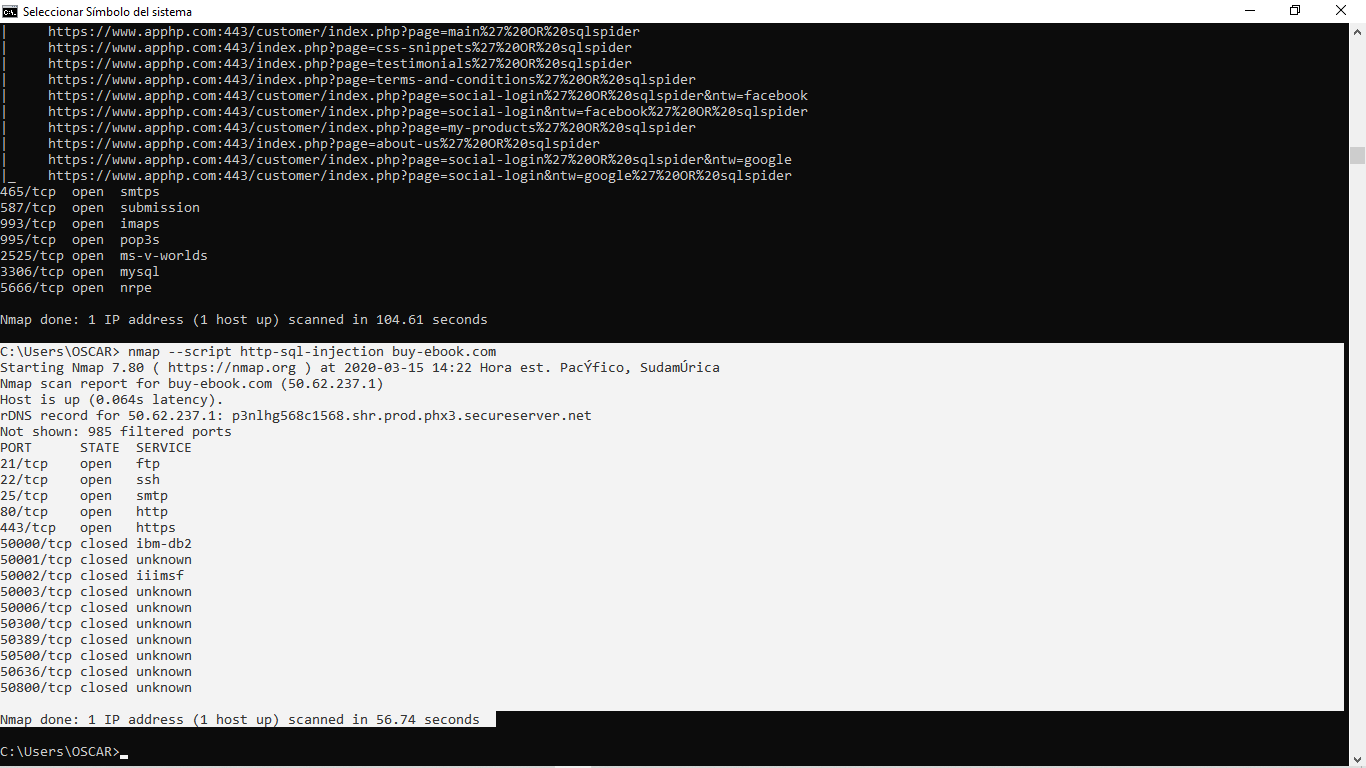
En la página securityhakiabs.net, devuelve sin ningún error encontrado en los puertos.



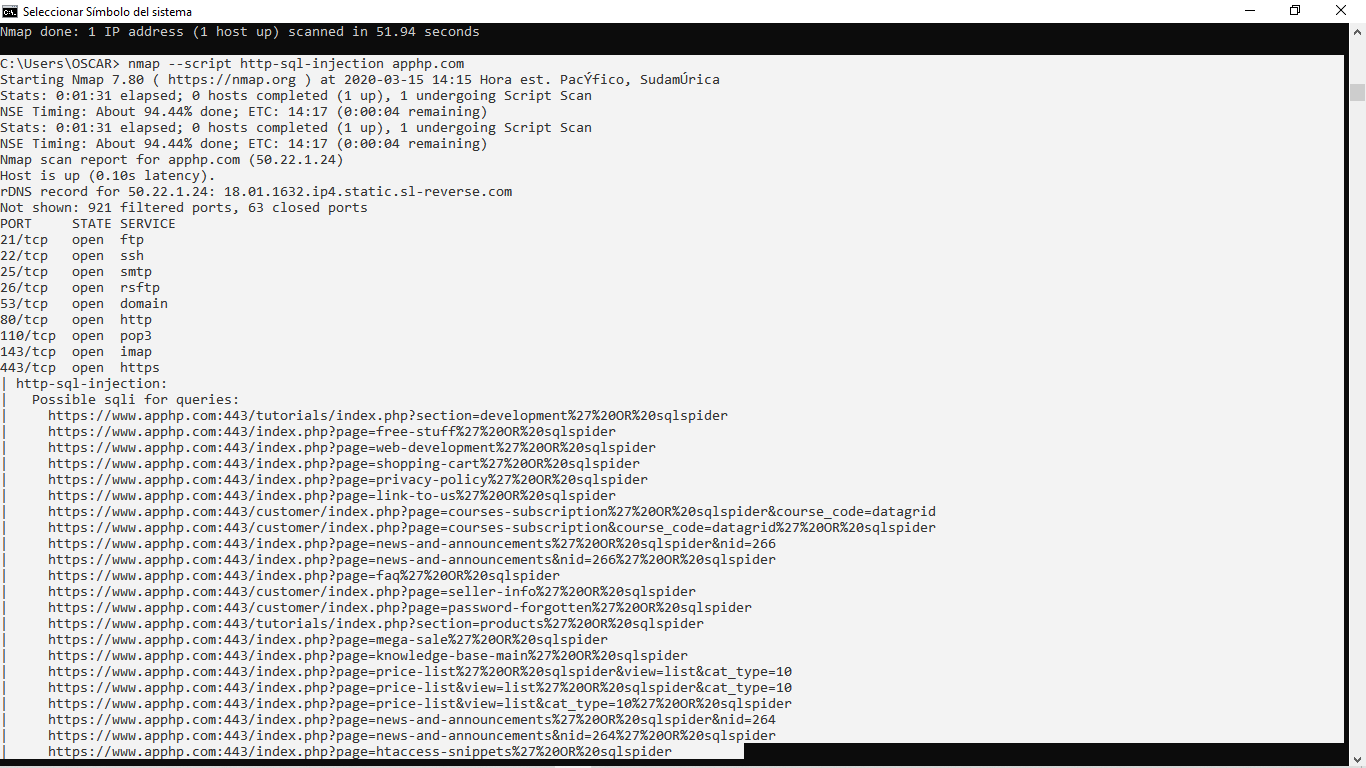
En la página Zombo.com, devuelve sin ningún error encontrado en los puertos.



En la página home.mcom.com, devuelve sin ningún error encontrado en los puertos.



En la página buy-ebook.com, devuelve sin ningún error encontrado en los puertos.

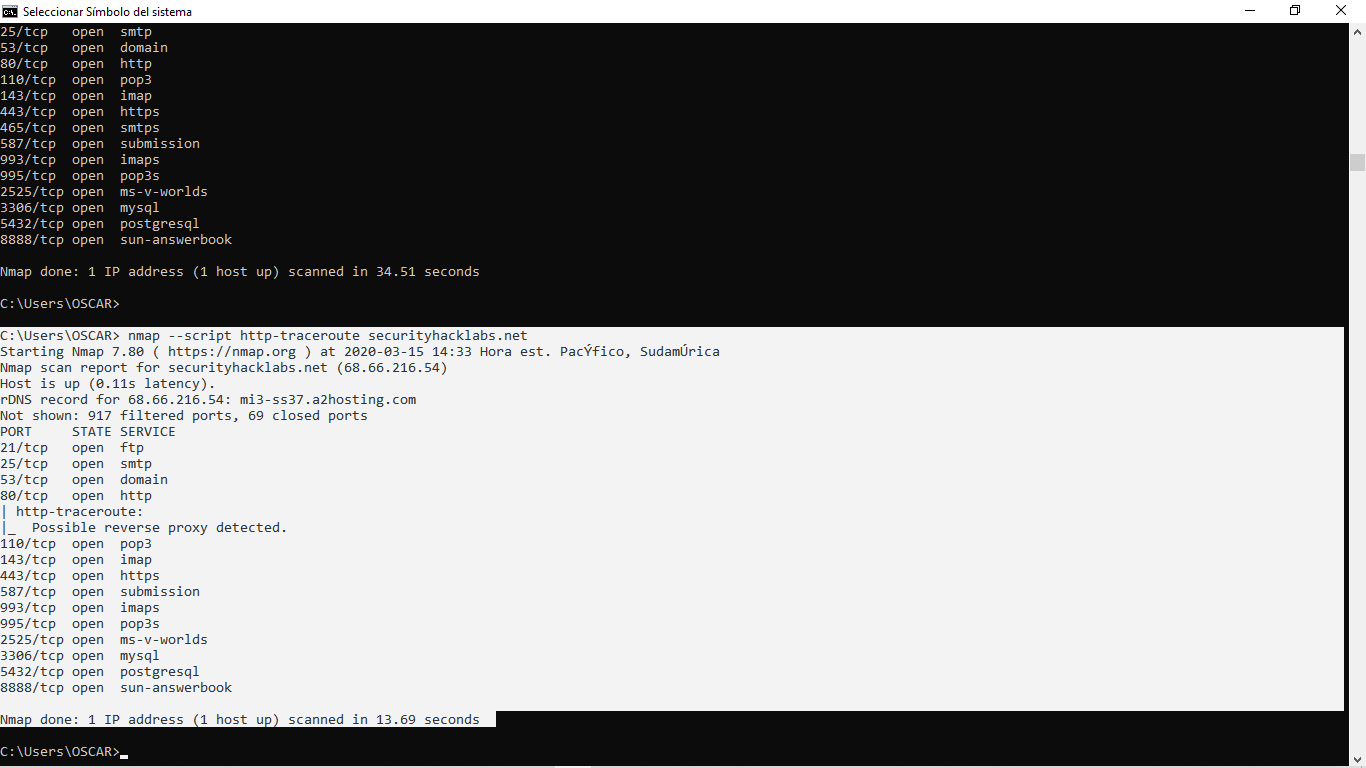


 En la página apphp.com, devuelve posibles queries que vulneren en el puerto 433.

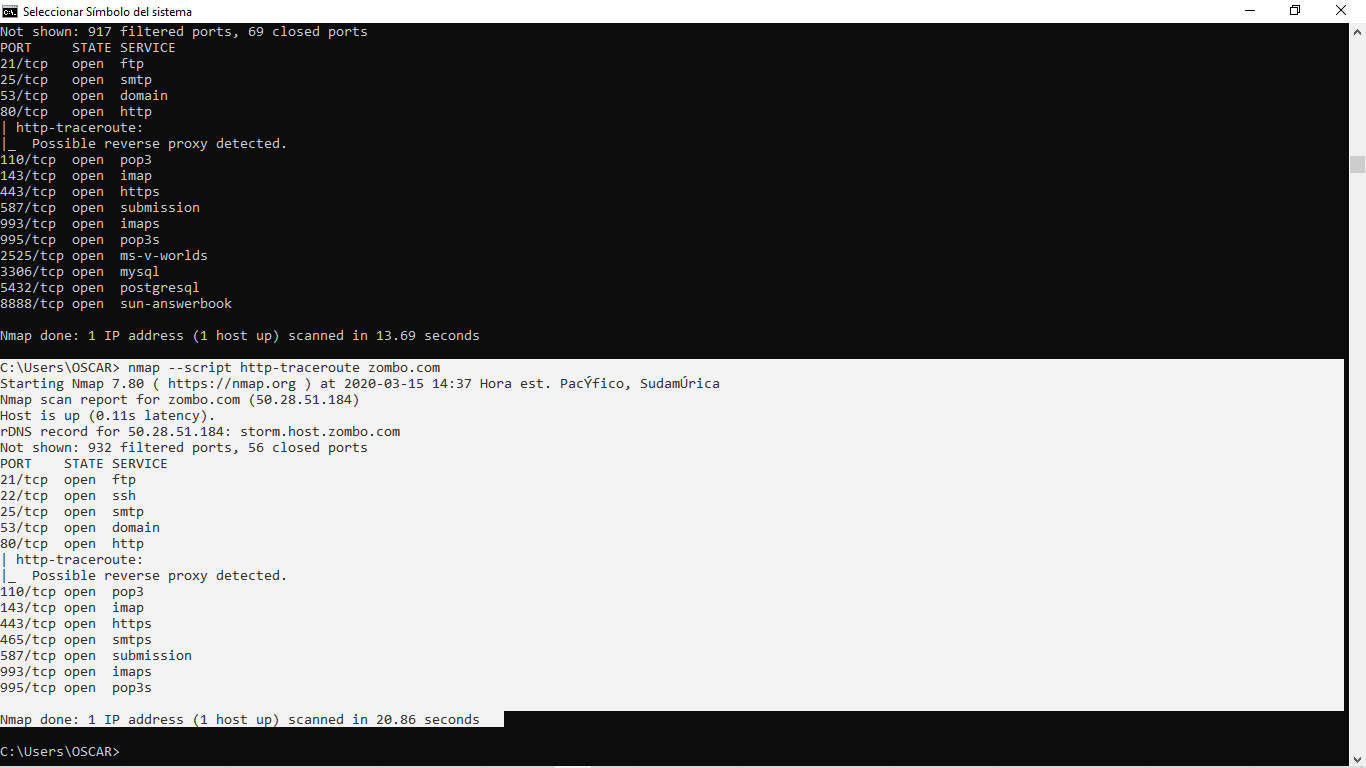
## **Scrip http-traceroute**

El script consiste en enviar solicitudes http con valores de encabezados http que varían entre 0-2 un spider a los servidores http de una url. Buscando anomalía en cualquier respuesta.

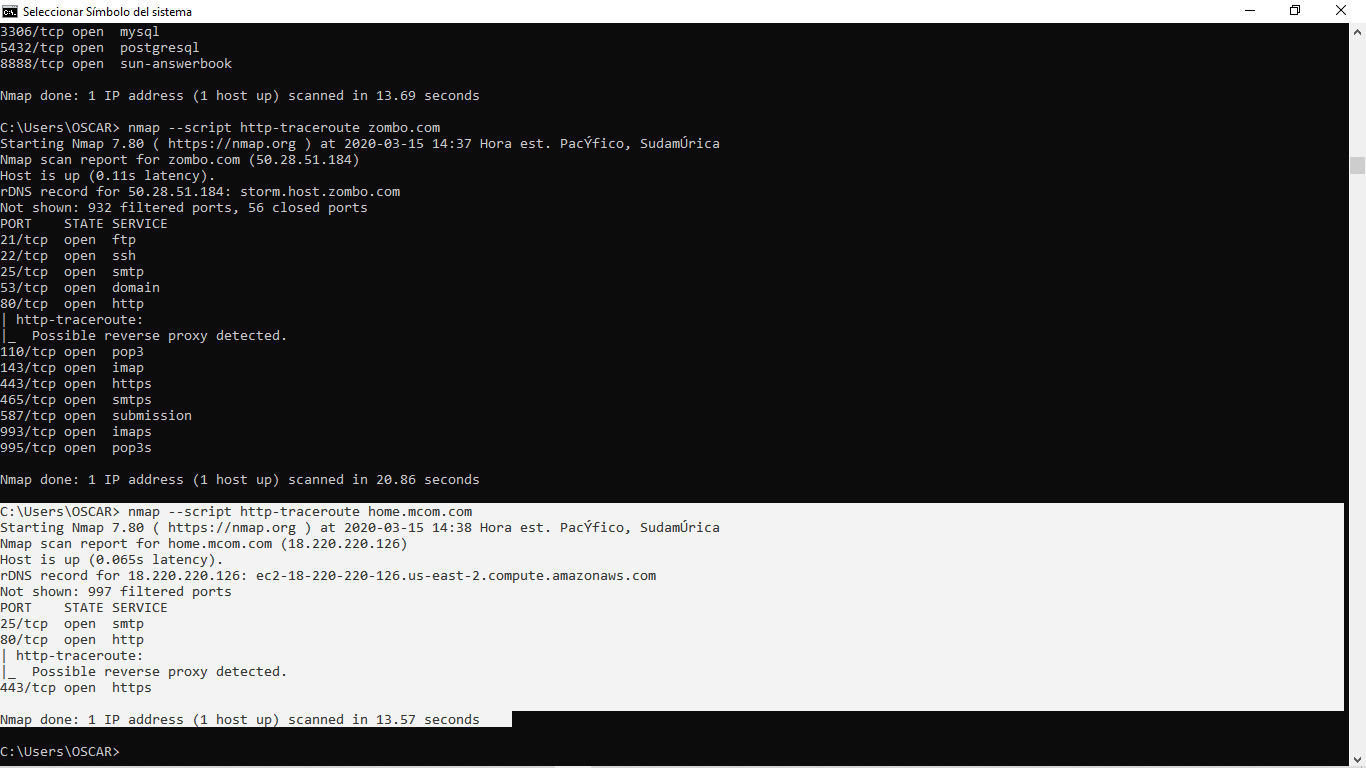
Posibles argumentos para especializar el script: http-traceroute.path, http-traceroute.method, slaxml.debug, http.host, http.max-body-size, http.max-cache-size, http.max-pipeline, http.pipeline, http.truncated-ok, http.useragent, smbdomain, smbhash, smbnoguest, smbpassword, smbtype, smbusername.



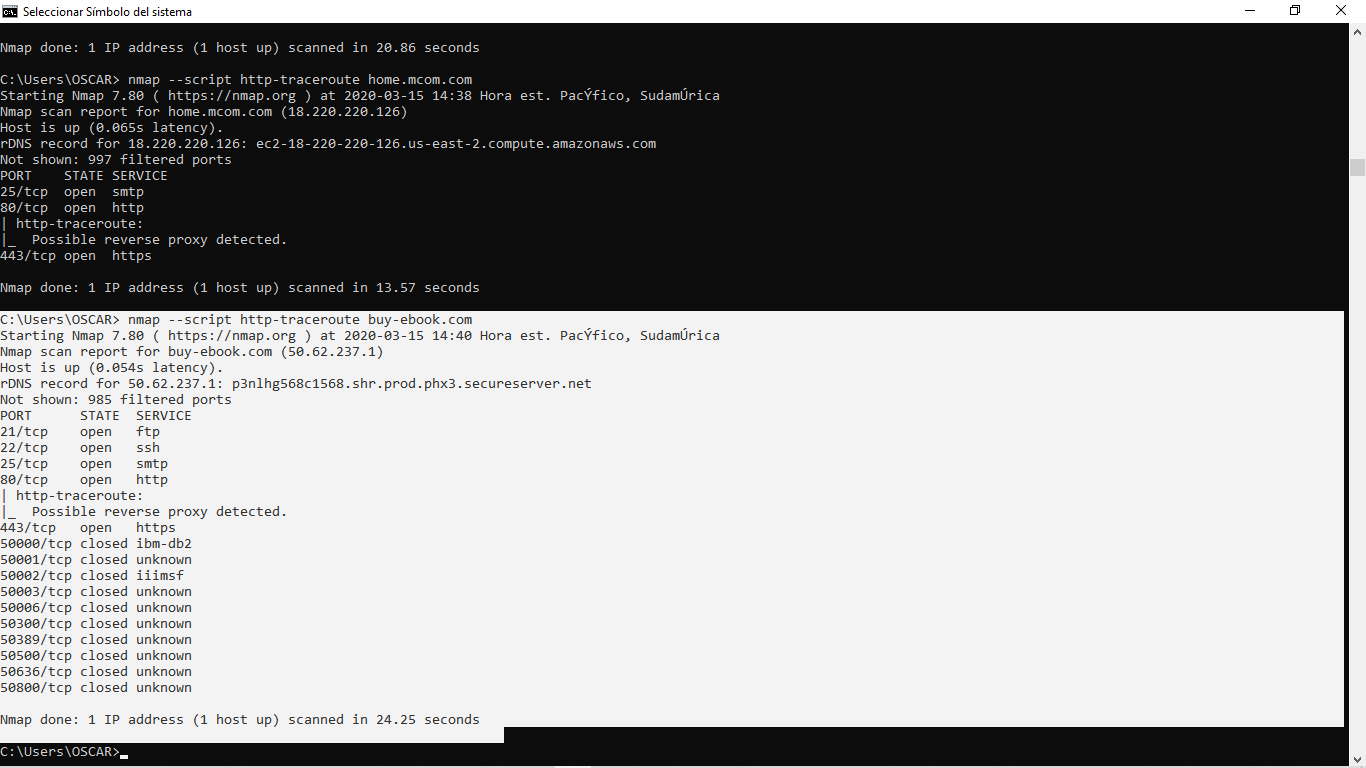
En la página securityhacklabs.net, devuelve una posible vulnerabilidad en el proxi en el puerto 80.



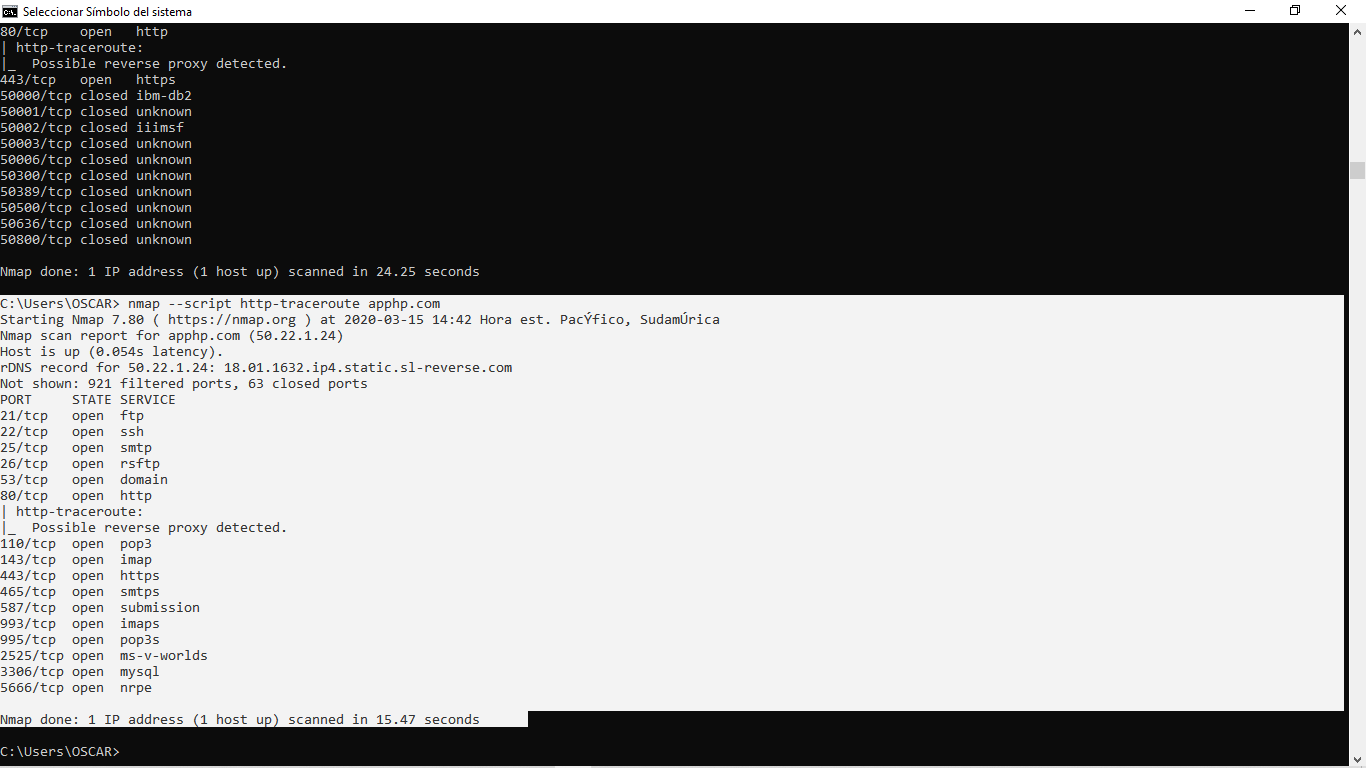
En la página Zombo.com, devuelve una posible vulnerabilidad en el proxi en el puerto 80.



En la página homr.mcom.com, devuelve una posible vulnerabilidad en el proxi en el puerto 80.



En la página buy-ebook.com, devuelve una posible vulnerabilidad en el proxi en el puerto 80.



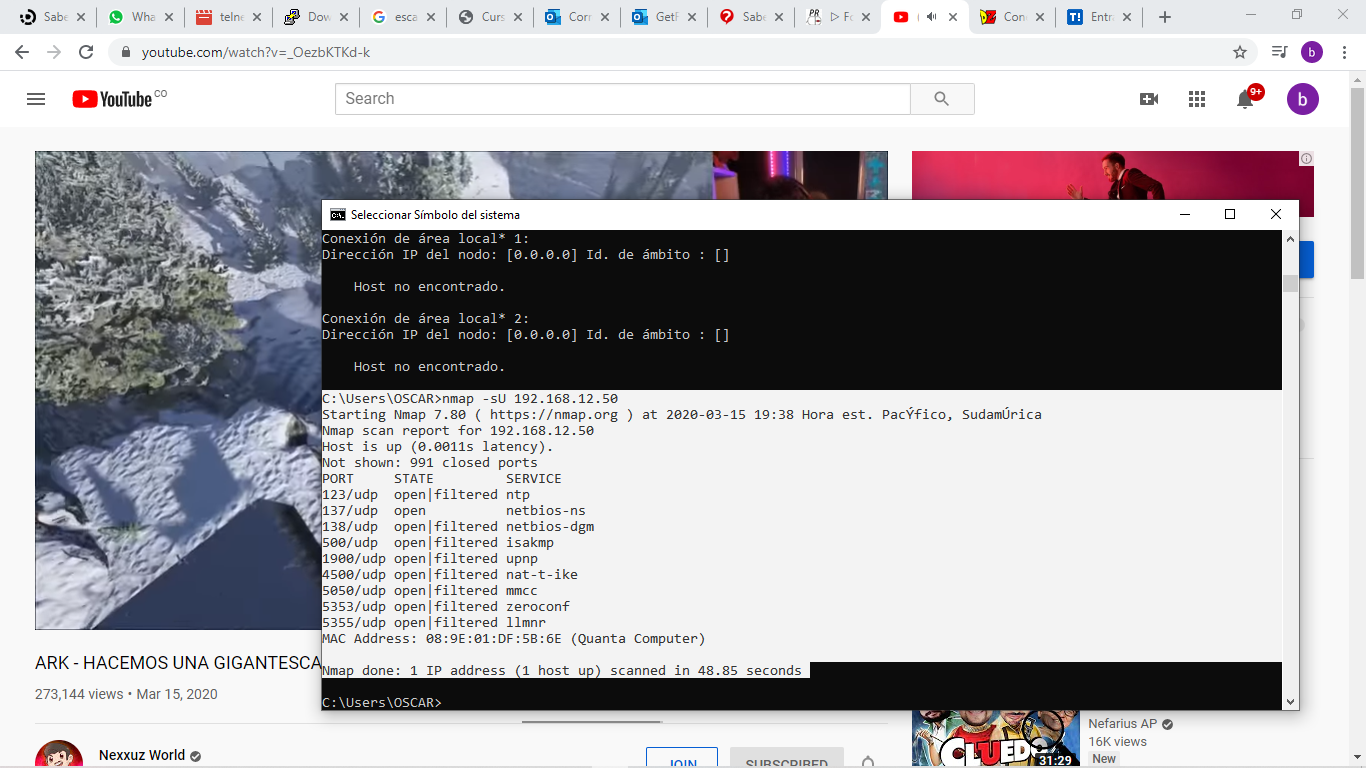
En la página apphp.com, devuelve una posible vulnerabilidad en el proxi en el puerto 80.

# PUNTO B

comunicación entre una máquina cliente y servidor

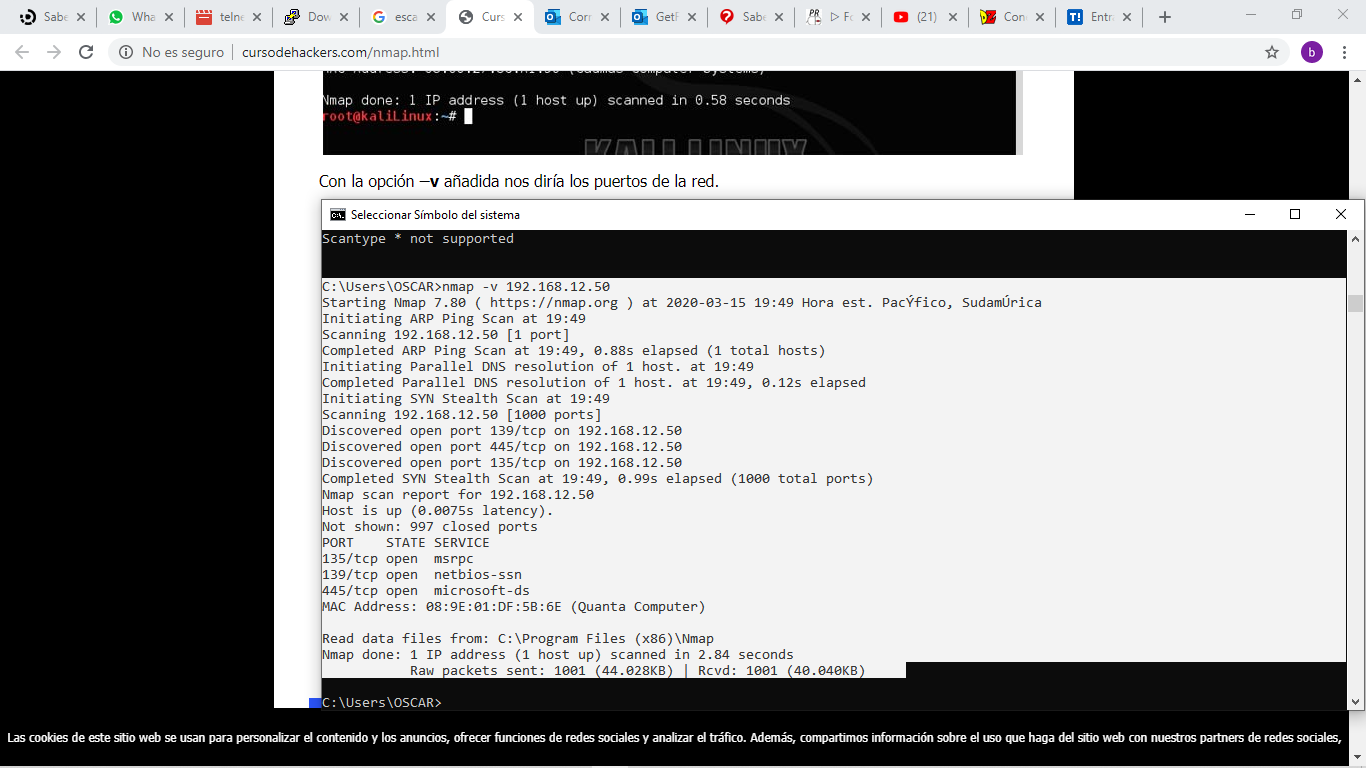
## **nmap -Su**

Escanea puertos y les envía peticiones para confirmar su estado y el servicio que esta prestando. Importante resaltar que enfatiza en los puerto con protocolo udp.



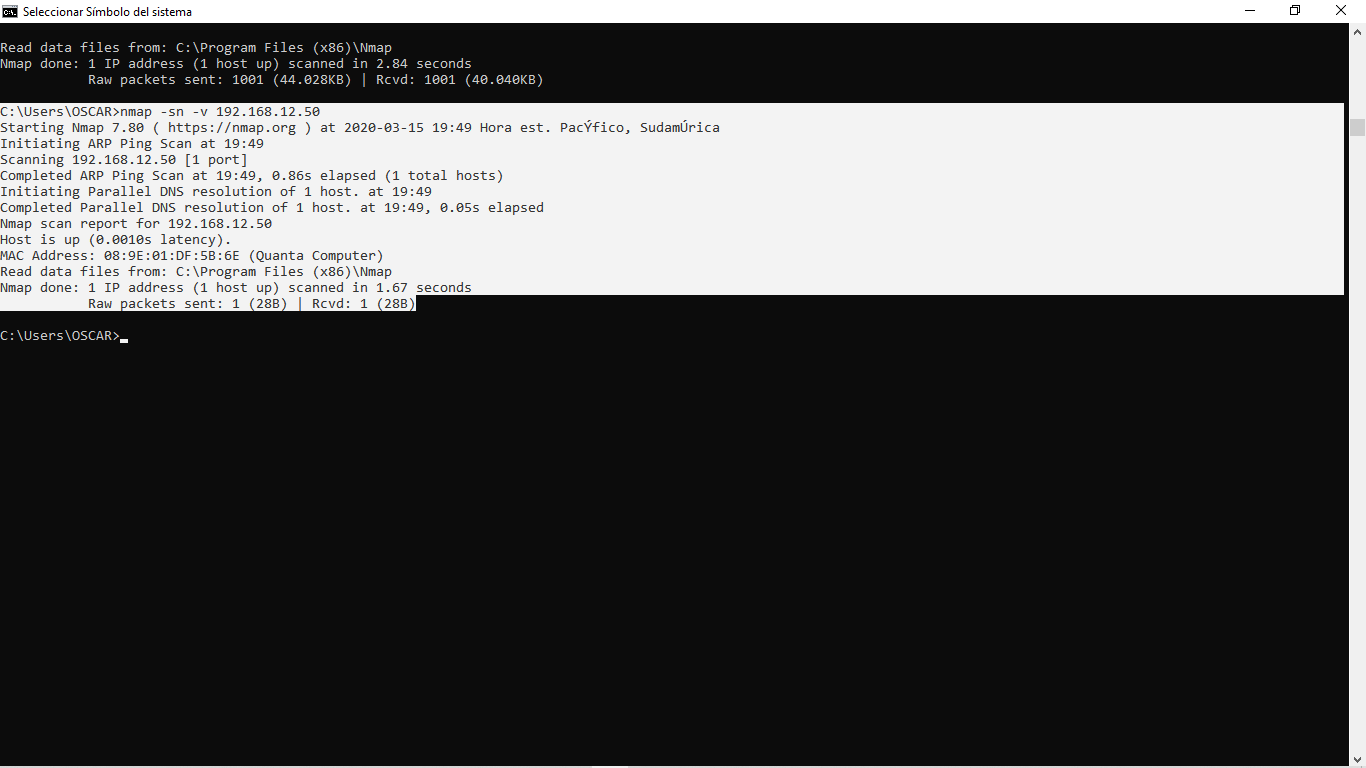
## **nmap -v**

Escanea puertos y les envía peticiones para confirmar su estado y el servicio que esta prestando. Importante resaltar que enfatiza en los puerto con protocolo tcp.



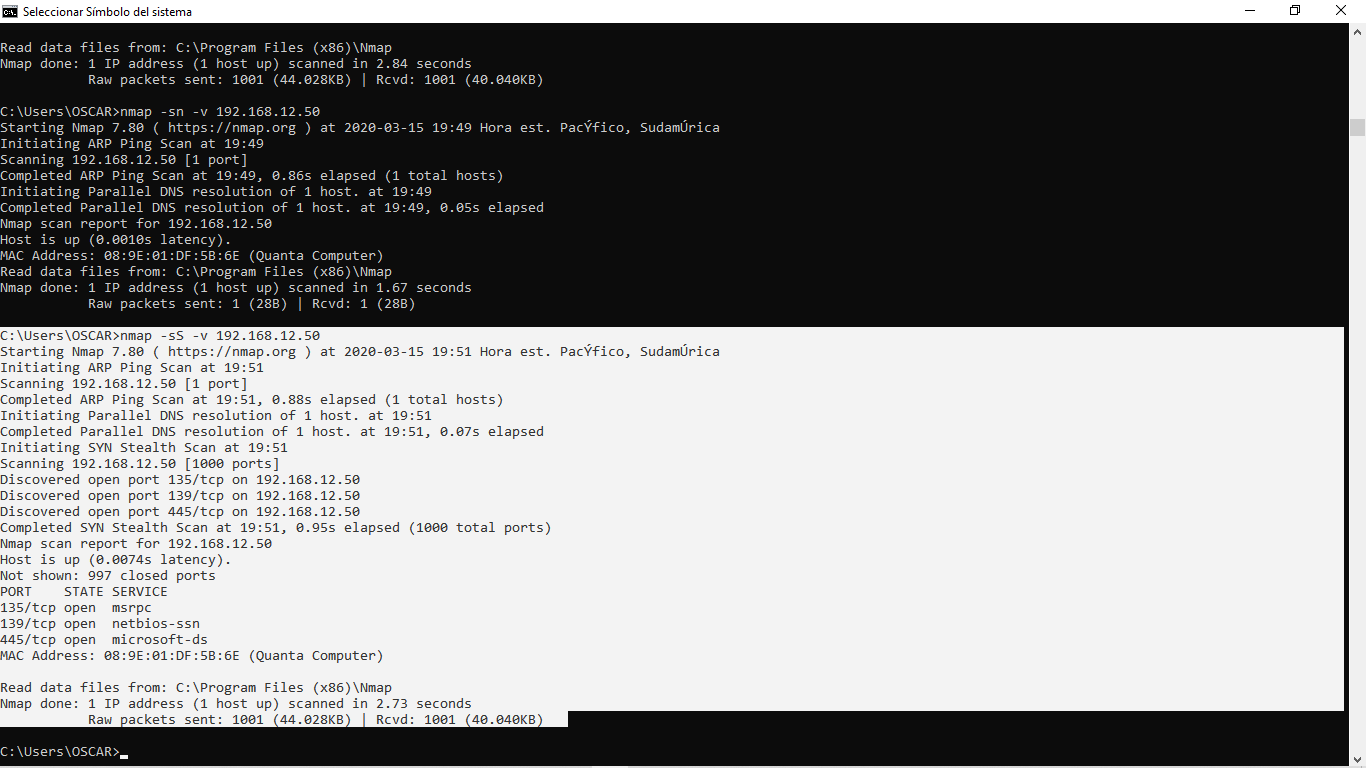
## **nmap -sn -v**

Devuelve la cantidad de maquinas en una red, en este caso solo encontrara 1 host. Por lo que solo reconoce la maquina cliente. El parámetro es una búsqueda mas detallada.



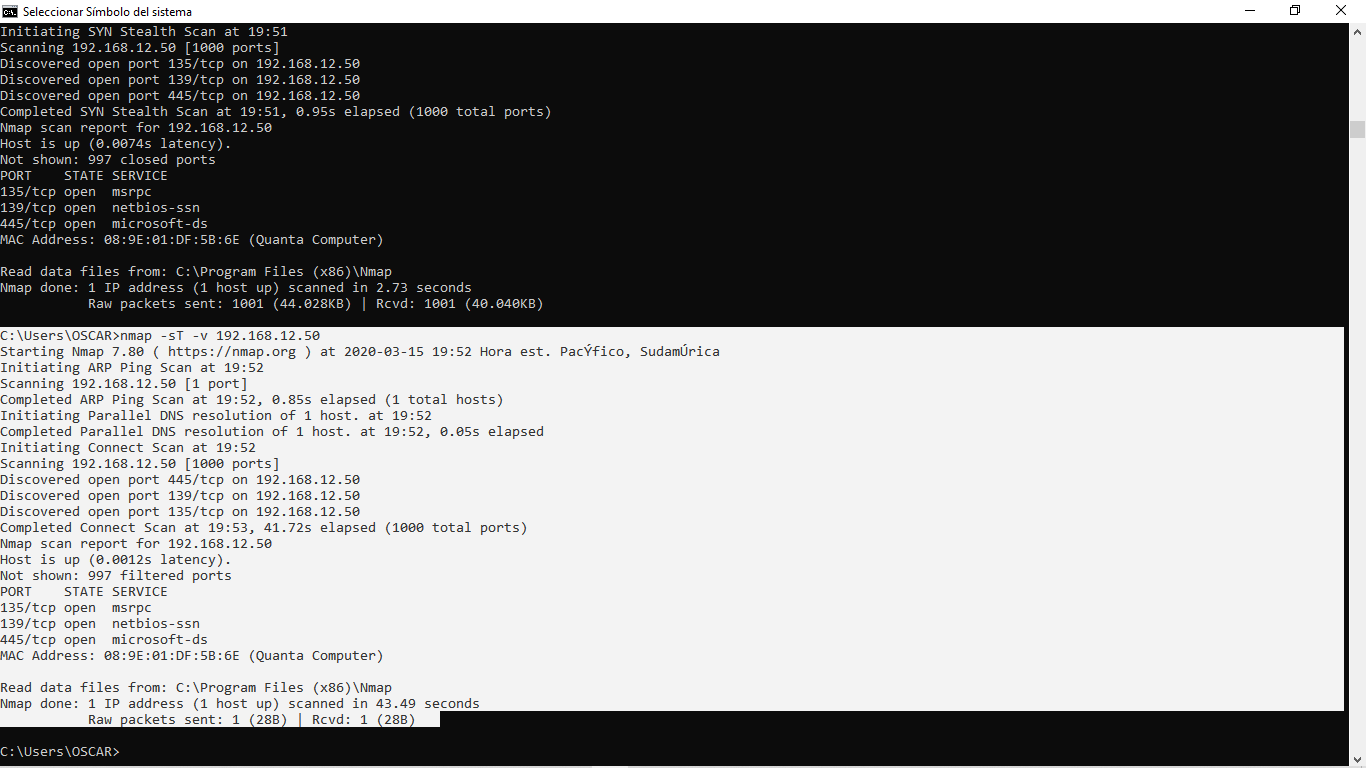
## **nmap -sS -v**

nos permite visualizar los puertos abiertos en una maquina dentro de la red. Con su corresponde servicio, protocolo y de a que maquina corresponden (una dirección ip).



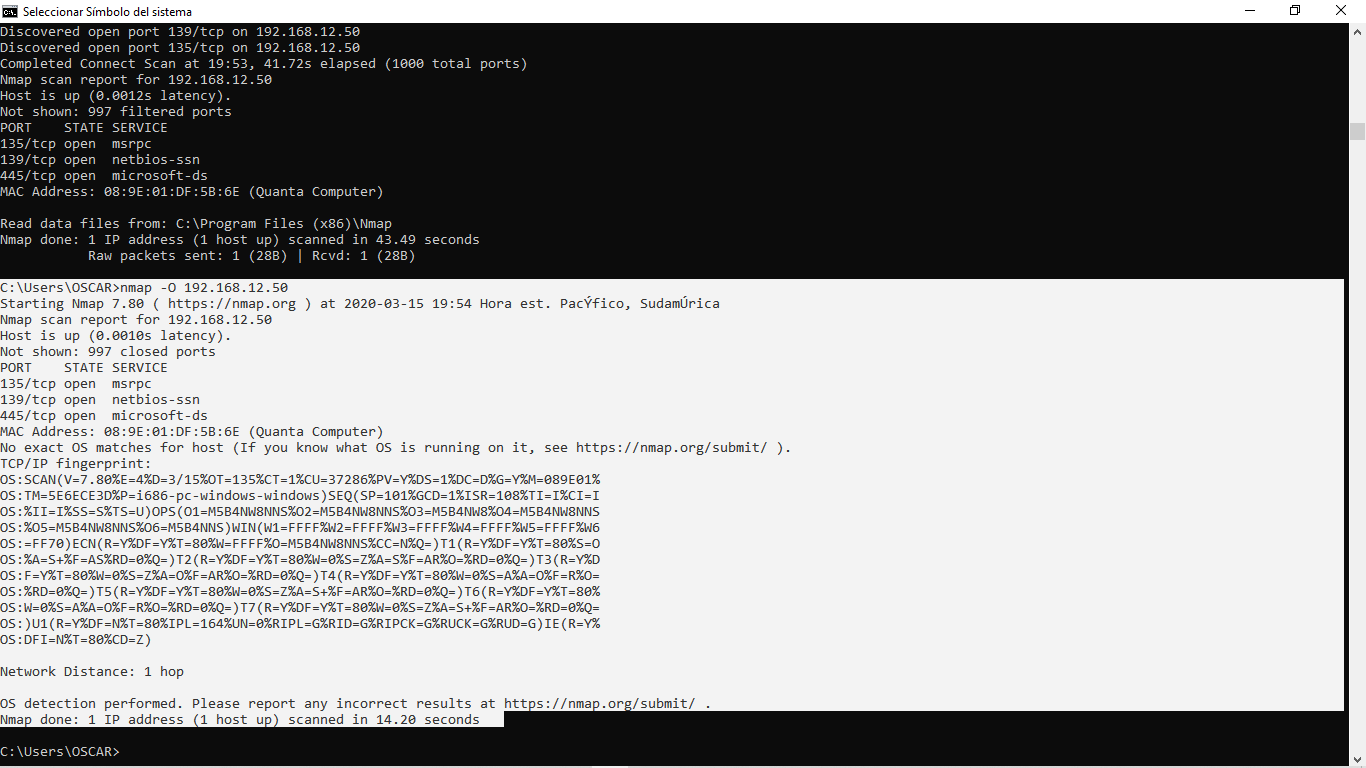
## **nmap -sT -v**

De igual manera nos permite analizar los puertos de maneta mas detenida sin embargo el realizar el escaneo, puede estar expuesto a quedar en los logs, dejando así una evidencia del escaneo.



## **nmap -O**

Nos muestra el sistema operativo de la víctima, el cual puede evidenciarse en este caso en el puerto 445



# BIBLIOGRAFIA

<https://nmap.org/nsedoc/>

<https://securityhacklabs.net/articulo/los-5-scripts-mas-intrusivos-y-avanzados-de-nmap-que-deberia-conocer>

<http://www.cursodehackers.com/nmap.html>