OWASP LATAM TOUR 2014

OWASP
LATAM TOUR
2014

NMAP WEB HACKING 101

WALTER CUESTAS AGRAMONTE

@WCU35745

WCUESTAS@OPEN-SEC.COM

Derechos de Autor y Licencia

DESCARGO DE RESPONSABILIDAD

Esta presentación tiene como propósito proveer unicamente información. No aplicar este material ni conocimientos sin el consentimiento explícito que autorice a hacerlo. Los lectores (participantes, oyentes, videntes) asumen la responsabilidad completa por la aplicación o experimentación de este material y/o conocimientos presentados. El(los) autor(es) quedan exceptuados de cualquier reclamo directo o indirecto respecto a daños que puedan haber sido causado por la aplicación de este material y/o conocimientos expuestos.

La información aquí expuesta representa las opiniones y perspectivas propias del autor respecto a la materia y no representan ninguna posición oficial de alguna organización asociada.

Ethical Hacking

Análisis de Incidentes

Auditoría de Configuración

Revisión de Seguridad del Código Fuente de Aplicaciones

They run automated tools, We have ETHICAL HACKERS

OFFENSIVE security OSCP

C)PTC™ CERTIFIED PENETRATION TESTING CONSULTANT

C)PTE™ CERTIFIED PENETRATION TESTING ENGINEER

C|EH™ Certified Ethical Hacker

C)PEH™ CERTIFIED PROFESSIONAL ETHICAL HACKER

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL CISSP®

OSEH OP3N-53C 37H1C4L H4CK3R

OWASP LATAM TOUR 2014

http://www.owasp.org

OWASP Open Web Application Security Project

El team...

Experiencia

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

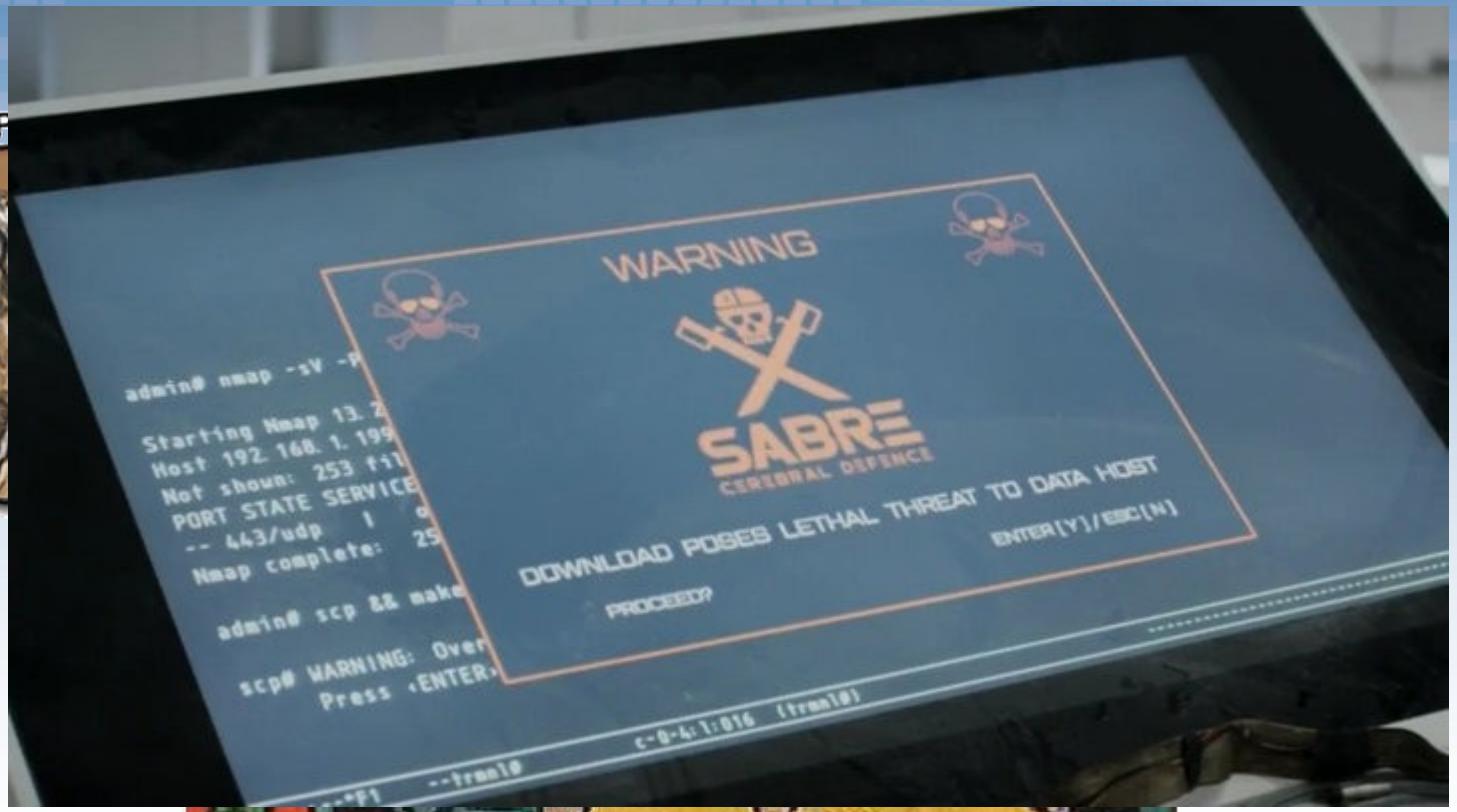
Greetings Mauricio,

Bizagi has confirmed the vulnerabilities and plans to release patches in June. This would be beyond the standard 45-day publication date, but it is common for us to delay publication until a patch is released. As the original vulnerability reporter, it is your choice whether we delay publication or stick to the standard 45-day disclosure date. Is it acceptable with you if we delay publishing the vulnerability note until the patch is released?

Best regards,

Vulnerability Analysis Team
==========
CERT Coordination Center
www.cert.org / cert@cert.org / Hotline: 1-412-268-7090
==========
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.5 (GNU/Linux)

NMAP ?


WARNING
SABRE
CEREBRAL DEFENCE
DOWNLOAD POSES LETHAL THREAT TO DATA HOST
ENTER(Y)/ESC(N)
PROCEED?
admin# nmap -sV
Starting Nmap
Host 192.168.1.199
Not shown: 253 filt
PORT STATE SERVICE
-- 443/udp
Nmap complete:
admin# scp && make
scp# WARNING: Over
Press <ENTER>
quickmeme.com

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 (próximo “chapter meeting” 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

NSE : Para web

- ls ***web*** ***http*** | wc -l
  - 105
- Cubren todo el “ciclo clásico” del hacking
  - Aunque no hagan todo

Footprint (fingerprint)

```
[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)

```
$ nmap -v -p 80 --script http-xssed.nse www.info          online.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          online.org (                ) [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          online.org (            ) [1 port]
Discovered open port 80/tcp on
Completed Connect Scan at 11:04, 0.20s elapsed (1 total ports)
NSE: Script scanning .
Initiating NSE at 11:04
Completed NSE at 11:04, 2.33s elapsed
Nmap scan report for www.info          online.org (                )
Host is up (0.18s latency).
rDNS record for                : .com
PORT   STATE SERVICE
80/tcp open  http
| http-xssed:
|
|     UNFIXED XSS vuln.
|
|       http://www.info          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%3CB
R%3E%3CBR%3E%3CBR%<br>3E%3CBR%3E%3CBR%3E%3CBR%3E%3CBR%3E%3CBR%3E
|
```

```
[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

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

Starting Nmap 6.46 ( http://nmap.org ) at 2014-04-26 10:07 PET
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Parallel DNS resolution of 1 host. at 10:07
Completed Parallel DNS resolution of 1 host. at 10:07, 0.21s elapsed
Initiating Connect Scan at 10:07
Scanning www.[redacted].pe ([redacted]) [1 port]
Discovered open port 80/tcp on [redacted]
Completed Connect Scan at 10:07, 0.01s elapsed (1 total ports)
NSE: Script scanning [redacted].
Initiating NSE at 10:07
Completed NSE at 10:07, 4.42s elapsed
Nmap scan report for www.[redacted].pe ([redacted])
Host is up (0.012s latency).
PORT   STATE SERVICE
80/tcp open  http
| http-waf-detect: IDS/IPS/WAF detected:
|_www.[redacted].pe:80/?p4yl04d3=<script>alert(document.cookie)</script>

NSE: Script Post-scanning.
Read data files from: /usr/local/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.84 seconds
```

Enumeración

```
[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
```

```
[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
```

Enumeración

```
[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
```

Búsqueda de

```
[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

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

Starting [illegible]
NSE: Loa[illegible]
NSE: Scr[illegible]
Initiat[illegible]
Complete[illegible]
Initiat[illegible]
Scanning[illegible]
Discover[illegible]
Complete[illegible]
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

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

Penetración (Explotación/Ataques)

- http-axis2-dir-traversal.nse
- http-barracuda-dir-traversal.nse
- http-brute.nse
- http-cors.nse
- http-default-accounts.nse
- http-dombased-xss.nse
- http-fileupload-exploiter.nse
- http-form-brute.nse
- http-passwd.nse
- http-phpmyadmin-dir-traversal.nse
- http-slowloris.nse
- http-vuln-cve2009-3960.nse
- http-vuln-cve2010-0738.nse
- http-vuln-cve2010-2861.nse
- http-vuln-cve2011-3192.nse
- http-vuln-cve2011-3368.nse
- http-vuln-cve2012-1823.nse
- http-vuln-cve2013-0156.nse
- http-vuln-zimbra-lfi.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

Datos Adicionales

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

OWASP

Open Web Application Security Project

Perú Chapter

Open-Sec

They run automated tools, We have ETHICAL HACKERS