

nmap

Nmap

Obtener hosts vulnerables como intermediario

```
nmap -O -v -sS|sT|sA|sW|sM objetivo -oA objetivo.result
```

Buscar los hosts vulnerables en el resultado

```
grep "IP ID" objetivo.result.gnmap | perl -pe 's/Host:([^\t]+).*IP ID  
Seq:([^\t]+)/$1 $2/'
```

Realizar ping a través de un intermediario

```
nmap -PN -p- -sI intermediario destino
```

Scripts para Nmap (NSE Nmap Script Engine)

Los scripts hay que copiamos en :

- Linux - /usr/share/nmap/scripts/ or /usr/local/share/nmap/scripts/
- OSX - /opt/local/share/nmap/scripts/
- Windows - c:\Program Files\Nmap\Scripts

Scripts para nmap

- <https://github.com/cldrn/nmap-nse-scripts>
- <http://www.computec.ch/projekte/vulscan/>.

para determinar si ha sido parcheado o no contra CVE2017-010.

Descargamos el script de

<https://raw.githubusercontent.com/cldrn/nmap-nse-scripts/master/scripts/smb-vuln-ms17-010.nse>

Ejecutamos :

```
nmap -sC -p445 --open --max-hostgroup 3 --script smb-vuln-ms17-010.nse  
X.X.X.X/X
```

Vulscan

<http://www.compute.ch/projekte/vulscan/> Vulscan es un script que permite usar nmap como un escaneador de vulnerabilidades, haciendo uso de varias bases de datos offline en formato csv. Actualmente usa las siguientes bases de datos:

- scipvuldb.csv - <https://vuldb.com>
- cve.csv - <http://cve.mitre.org>
- osvdb.csv - <http://www.osvdb.org>
- securityfocus.csv - <http://www.securityfocus.com/bid/>
- securitytracker.csv - <http://www.securitytracker.com>
- xforce.csv - <http://xforce.iss.net>
- exploitdb.csv - <http://www.exploit-db.com>
- openvas.csv - <http://www.openvas.org>

Para instalar Vulscan basta con copiar los ficheros del proyecto a un directorio vulscan dentro del directorio de scripts del nmap → Nmap\scripts\vulscan*

Como las

Referencias

- <http://calderonpale.com/>
- <http://abdulet.net/>
- <http://conocimientolibre.wordpress.com/2007/06/30/nmap-a-fondo-escaneo-de-redes-y-hosts/>
- <http://xora.org/2013-4-scripts-de-nmap-indispensables-para-vulnerabilidades-del-2012/>
- <http://www.hackplayers.com/2017/05/como-detectar-pcs-vulnerables-a-wannacry.html>

From:

<http://intrusos.info/> - **LCWIKI**

Permanent link:

<http://intrusos.info/doku.php?id=seguridad:herramientas:nmap&rev=1496050651>

Last update: **2023/01/18 14:20**

