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:([^:]+)/$1 $2/’
```

Realizar ping a través de un intermediario

<shx>nmap -PN -p- -sI intermediario destino </shx>

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

Lo 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

Ejecutamos :

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

Scripts

https://github.com/cldrn/nmap-nse-scripts

Referencias

- 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:
https://intrusos.info/ - **LCWIKI**

Permanent link:
https://intrusos.info/doku.php?id=seguridad:herramientas:nmap&rev=1495801893

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