nmap

parámetros

- -sS : escanea los puertos más normales o los difinidos en `services`
- -p : escanea un puerto determinado (50), un rango (50-60) o todos, poniendo un guión (-p-)
- -Tx : establece el periodo de tiempo que deja pasar para escanear un dispositovo para evitar ser detectado y que el firewall nos mande información falsa. De más espaciado a menos:
  - T0: paranoid
  - T1: sneaky
  - T2: polite
  - T3: normal
  - T4: aggresive
  - T5: insane

scripts

Uso de scripts para escaneos varios:

- Auth
  - la herramienta detecta (primer recuadro azul) el ingreso de usuarios anónimos (sin requerir usuario y contraseña). Del mismo modo, en el segundo recuadro azul (recuadro inferior) nos muestra el listado de usuarios con permisos de superusuario (acceso root) en MySQL que no poseen contraseña.
  - ```
    sudo nmap -f -sS -sV -Pn --script auth <IP>
    ```
- default
  - ```
    sudo nmap -f -sS -sV -Pn --script default <IP>
    ```
- safe
  - El script safe se podría utilizar cuando queremos ejecutar secuencias de comandos que son menos intrusivas para la víctima, de manera que será menos probable que provoquen la interrupción de algunas aplicaciones.
  - ```
    sudo nmap -f --script safe <IP>
    ```
- Vuln
  - permite identificar alguna de las vulnerabilidades más conocidas en el sistema.
  - ```
    sudo nmap -f --script vuln <IP>
    ```
- All (poco recomendable)
  - ```
    sudo nmap -f --script all <IP>
    ```
- Existen otros:
  - Discovery: recupera información del target o víctima
  - External: script para utilizar recursos externos
  - Intrusive: utiliza scripts que son considerados intrusivos para la víctima
  - malware: revisa si hay conexiones abiertas por códigos maliciosos o backdoors
  - https://nmap.org/nsedoc/scripts/
    ```

/via: https://www.welivesecurity.com/la-es/2023/06/14/auditando-nmap-scripts-escanear-vulnerabilidades/

+ info

- https://hackertarget.com/nmap-cheatsheet-a-quick-reference-guide/

cut&paste

- scan de puertos:

```
nmap -sS -sV -P0 -O <ip o dominio>
```

```
nmap -sS <ip o dominio> -> scan de los puertos más normales o los definidos en ''services''
```

- hosts activos de una red:

```
nmap -sP <ip_range>
```

- hosts con puerto activo (en este caso, AFP apple):

```
nmap -p 548 <ip> -Pn -n
```

- Scan a través de proxies (ver lista más abajo):

```
# nmap -sS -sV -P0 -O --proxies "http://199.193.255.160:3128,http://64.20.45.139:8080,http://64.20.54.211:8080" www.torrelles.cat
```

- puertos abiertos:

```
sudo nmap -sT -O localhost
```

- puertos abiertos a web:

```
nmap -v -A (Sitio web)
```

proxies

- http://proxylist.hidemyass.com/search-1305348#listable
- https://www.sslproxies.org/