Nmap

Nmap és un programa de codi obert per la rastreja de ports. S'usa per avaluar la seguretat de sistemes informàtics, així com per descobrir serveis o hosts en una xarxa informàtica, per això Nmap envia uns paquets definits a altres equips i n'analitza les respostes.

Pots descarregar la versió de Windows des de: https://nmap.org/download.html

Nmap disposa d'una interfície gràfica: Zenmap.

Pots veure totes les comandes introduint a la terminal:

```
nmap --help
```

Algunes comandes

Escanejar els ports oberts més freqüents d'un host: nmap [ip]

```
nmap 192.168.123.28
```

Escanejar un rang de ports d'un host: nmap -p [port o rang de ports] [ip]
Els ports d'un sistema operatiu s'enumeren del 0 al 65535. Per registrar-los tots podem fer:

```
nmap -p 0-65535 192.168.123.28
```

Escanejar un rang d'IPs: nmap [ip1]-[últim octet ip2]

```
nmap 192.168.123.1–255
```

Obtenir el sistema operatiu i serveis d'un host: nmap -a -v [ip]

```
nmap -Av 192.168.123.28
```

La forma d'identificar el SO és a través de la forma en què retorna els paquets enviats, de manera que no és totalment fiable.

Escaneig dels equips de la xarxa: nmap [ip]/[prefix xarxa]

```
nmap 192.168.123.0/24
```

ACTIVITATS

Utilitza **Wireshack** per monitoritzar els escanejos que realitza Nmap.

Fixa’t que amb l’opció per defecte i més ràpida: nmap -sS [ip]
Nmap envia únicament un paquet SYN i el host objectiu retorna SYN/ACK.

En canvi, amb la opció: nmap -sT [ip]
Nmap estableix una connexió TCP completa amb el host objectiu: SYN, SYN/ACK i ACK.

BIBLIOGRAFIA I WEBGRAFIA

«Hacker Target». https://hackertarget.com/nmap-tutorial/
«Proteger mi PC». https://protegermipc.net/2018/11/07/tutorial-y-listado-de-comandos-mas-utiles-para-nmap/