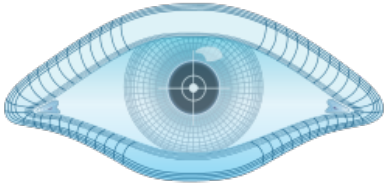
NMAP



NMAP es una herramienta para **escanear puertos abiertos, servicios, versiones, sistemas operativos…**

1.

INTRODUCCIÓN A NMAP

Introducción a Nmap

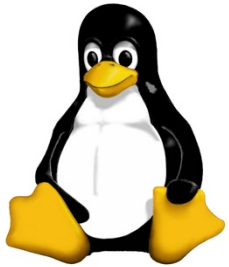
- Herramienta orientada a obtener información de los sistemas
- Imprescindible para auditores
- TCP y UDP

2.

INSTALACIÓN DE NMAP

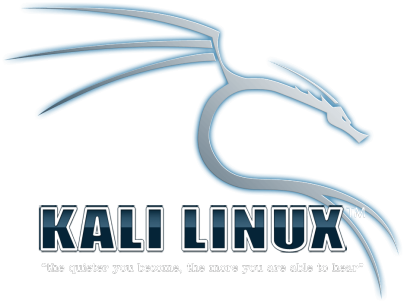
Herramienta multiplataforma y Open Source

https://nmap.org/download.html



PRÁCTICAS EN EL LABORATORIO

Kali Linux



Source Code compilation

> bzip2 -cd nmap-7.40.tar.bz2 | tar xvf -
> cd nmap-7.40
> ./configure
> make
> su root
> make install

3.

DESCUBRIMIENTO DE PUERTOS

- NMAP dispone de gran cantidad de opciones

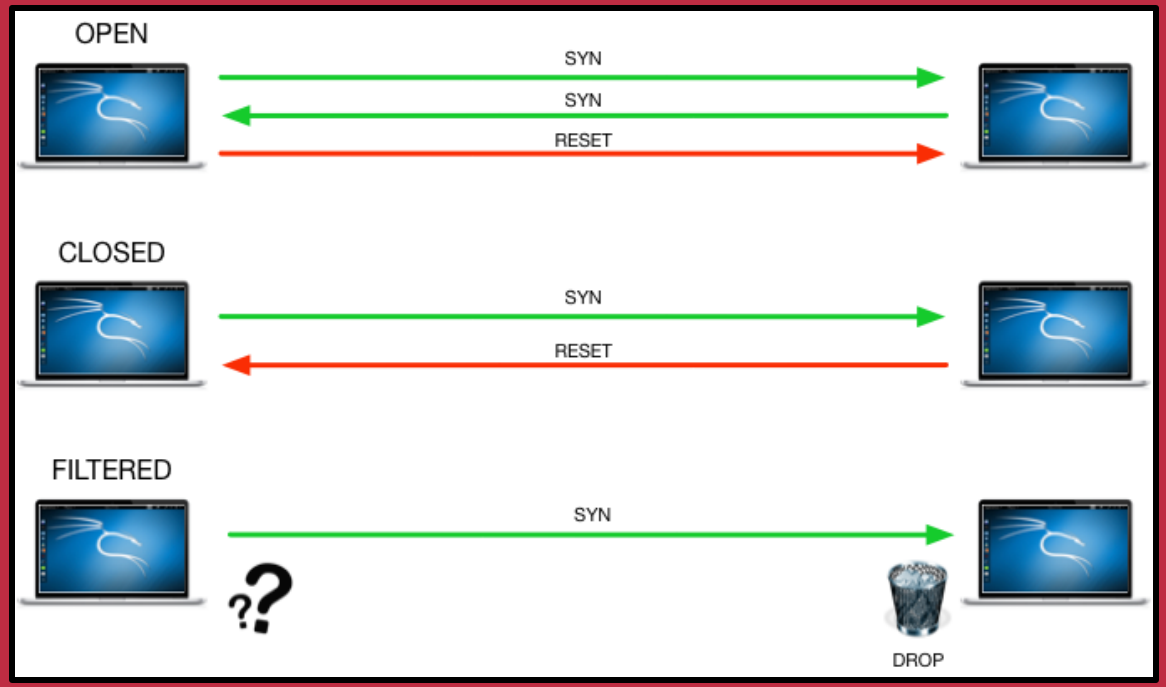
- Escaneo básico sobre equipo o red:

Equipo: *# nmap 172.16.0.132*
Red: *# nmap 172.16.0.0/24*

Posibles estados de los puertos:

- *Open*: puerto abierto a la espera de una conexión con un servicio tras él a la escucha.
- *Closed*: puerto accesible pero sin ninguna aplicación escuchando tras él.
- *Filtered*: Nmap no recibe respuestas y por tanto no puede establecer el estado, probablemente por la presencia de algún tipo de filtrado (firewall, IDS, etc.).

POSIBLES RESPUESTAS



- Filtrado de puertos

Por defecto, Nmap escanea los 1000 puertos más usados:
21 (ftp), 22 (ssh), 80 (http)...
Se puede seleccionar puertos y rangos de los mismos.

- ➢ Puertos concretos *# nmap –p 21,22,80 172.16.0.132*
- ➢ Rango de puertos *# nmap –p 20-100 172.16.0.132*
- ➢ Escaneos UDP *# nmap –p 53,123 -sU 172.16.0.132*
  (UDP o NTP)

- Distintas opciones

Existen muchas opciones para distintos escenarios:

- No usar Ping — *# nmap –PN 172.16.0.132*
- Deshabilitar la resolución inversa de nombres — *# nmap –n 172.16.0.132*
- Debug (-v/-vv…) — *# nmap –vv 172.16.0.132*

- Descubrimiento de servicios

Conocer qué servicio escucha detrás de un puerto.

➢ Versión del servicio usando los banners de respuesta *# nmap –sV 172.16.0.132*

➢ Intensidad del escaneo *# nmap –version-intensity 9 172.16.0.132*

Mayor intensidad → más pruebas → pero más visibles

➢ Sistemas Operativos *# nmap -O 172.16.0.132*

4.

OTROS ESCÁNERES

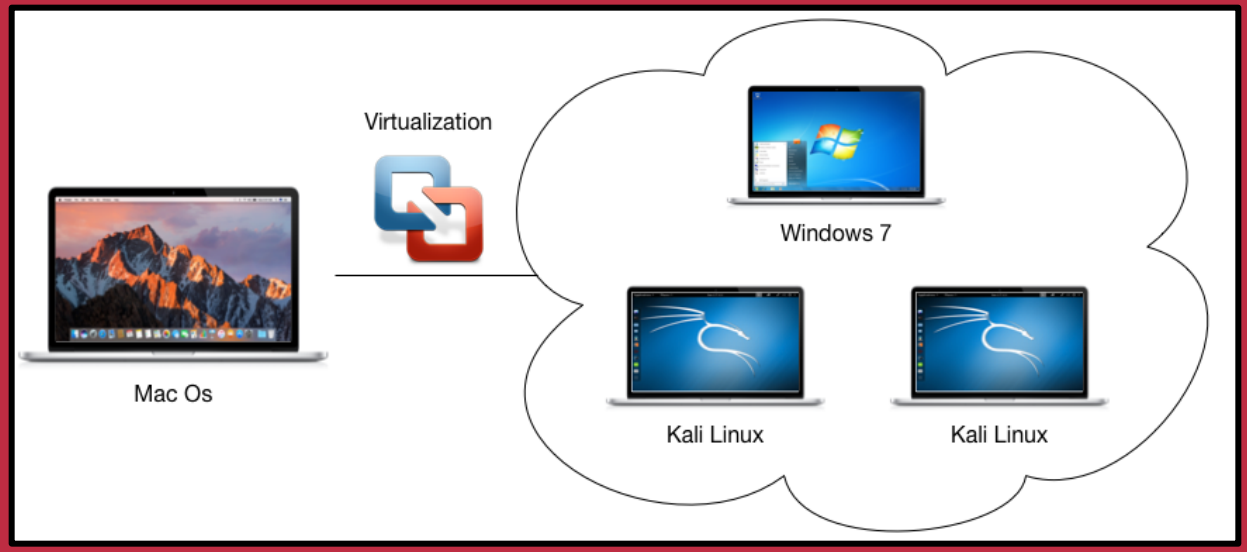
- Dos posibles alternativas

ZMAP (*https://zmap.io*)

- Escáner Open-Source orientado a redes grandes. Teóricamente podría escanear internet en una hora aproximadamente pero solo está orientado a IP v4.

MASSCAN (*http://tools.kali.org/information-gathering/masscan*)

- Teóricamente puede escanear internet en 6 minutos. Funciona parecido a otras herramientas como *scanrand*, *unicornscan* o *zmap*. Además de su velocidad es más flexible permitiendo rangos de direcciones IP y puertos.



LABORATORIO