Escaneo de Puertos.

Comando "nmap".

Como se sabe el protocolo TCP, funciona en base puertos.

Hay muchos programas comerciales que permiten "mirar" los "puertos abiertos" de un equipo.

Con "mirar", estamos diciendo escanear y con "puertos abiertos", nos estamos refiriendo a puertos que en los cuales posiblemente se está brindando un servicio (web, mail,etc.).

El comando de linux : nmap , permite de una manera muy sencilla realizar esto en modo texto.

Para ejecutar este comando es preferible ser root.

Vamos a decribir las opciones mas comunes.

- Tipeando nmap o nmap –help desde la terminal se pude tener un detalle de que hace este comando y sus opciones.
- La sintaxis básica sería: Usage: nmap [Scan Type(s)] [Options] {target specification}
- En Target specification , se puede indicar:
  - Hostnames, IP addresses, networks, etc. Ejemplo:
    - scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
- nmap -O x.x.x.x , permitiría obtener información sobre el Tipo de sistema Operativo que tiene el equipo con ip x.x.x.x.

Ejemplo:

Comando: nmap -O 192.168.0.90

Resultado:

Starting Nmap 5.00 (http://nmap.org) at 2012-10-17 17:53 ART

Interesting ports on 192.168.0.90:

Not shown: 998 closed ports PORT STATE SERVICE

111/tcp open rpcbind

631/tcp open ipp

MAC Address: 00:0D:87:0F:5D:C2 (Elitegroup Computer System Co. (ECS))

Device type: general purpose Running: Linux 2.6.X OS details: Linux 2.6.13 - 2.6.27

Network Distance: 1 hop

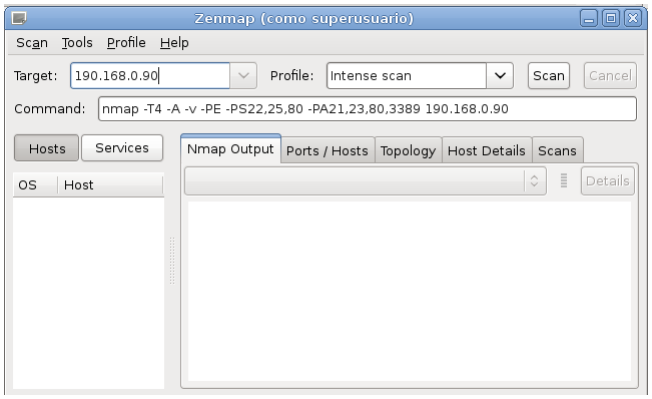
OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 3.16 seconds

- nmap -e x.x.x. , permite especificar la interfaz por la cual se realizará el escaneo de puerto.

- nmap -F x.x.x.x , permite un escaneo rápido (Fast).
- nmap -ttl 10 x.x.x.x , permite setear el campo TTL del Datagrama a el valor 10.
- nmap -v x.x.x.x , modo Verbose.
- nmap -open x.x.x.x , da un listado de los puertos posiblemente abiertos.
- Con la opción -exclude, se puede escluir un host del escaneo.
- Con la opción PS , se pude dar una lista de puertos: nmap -PS22,25.

Si se quiere algo mas gráfico existe el Zenmap, este sería una interfaz gráfica del nmap.



Podemos ver en el cuadro de texto de "Command" que el comando que ejecuta es el nmap, también se ven las opciones del comando:

-T4 -A -v -PE -PS22.25.80....etc

La información brindada es la misma que el nmap.

Para ejecutar esta aplicación se debería tener derechos de root , en caso contrario se vería un cartél como el siguiente: