ESCANEO DE SERVICIOS

En primer lugar deberemos conocer cuáles son los servicios que están corriendo en una maquina por que serán estos los principales puntos de entrada al sistema. Normalmente cada servicio que corre en una maquina tiene un puerto asignado por el cual se conecta con el resto de sistemas.

Para proceder a esta fase de reconocimiento utilizaremos una herramienta llamada nmap. Es el escáner de puertos por excelencia además de tener otras muchísimas más utilidades. La principal función que le daremos será la de obtener que puertos hay abiertos, y que servicios hay corriendo en estos.

Es una herramienta que se utiliza por línea de comandos. Para instalarla la descargaremos por la vía habitual del repositorio de paquetes de linux:

```
leurian@asus:~$ sudo apt-get install nmap
```

La herramienta es muy simple de utilizar. Solo tenemos que poner nmap seguido de las opciones de escaneo que queramos utilizar junto a la dirección IP a escanear. Es decir:

```
leurian@asus:~$ nmap -sV -O 8.8.8.8
```

Este comando nos proporcionará un listado con los puertos (Mas comunes) abiertos del sistema alojado en la dirección IP 8.8.8.8 . Como podéis ver le hemos puesto dos opciones. La primera -sV nos proporcionará los nombres de los servicios corriendo en cada puerto (de esta manera podremos buscar por la red que exploits son capaces de explotar estos servicios para poder acceder al sistema). La opción -O nos identificará de qué tipo de sistema operativo se trata (cuanto más antiguo es un sistema operativo más vulnerabilidades tiene). Por último otra opción a destacar seria –A que nos realiza un escaneo de puerto y del sistema operativo lo más detallado posible

Si no estamos muy acostumbrado a la línea de comandos (mal hecho, que mejor momento que este para hacerse con ella) podremos utilizar la interfaz gráfica de esta aplicación. Es muy intuitiva de usarla. Para instalarla podremos encontrarla en el repositorio de linux:

```
leurian@asus:~$ sudo apt-get install zenmap
```

Por último comentar que nmap es una muy potente herramienta que permite realizar gran cantidad de escaneos que serán explicados en el blog para todos aquellos que deseen más información, y como siempre recordaros que ante cualquier duda no dudéis en contactar con nosotros en info@highsec.es.