**Escaneadores de red (basados en NMAP)**

## **Las herramientas más usadas para la realización de un análisis de redes. Nmap, NBTscan y Netcat ¿Cuáles son sus principales beneficios?**

## **Existen herramientas de gran calidad que te ayudarán a realizar un análisis en la red de tu empresa de manera rápida. Esto te servirá para diagnosticar los sistemas informáticos y verificar que sea completamente seguro. También, es posible detectar cualquier error en el sistema, lo que te permitirá mejorar su funcionamiento.**

## **Para realizar su análisis, estas herramientas toman en cuenta los protocolos de internet y los sistemas operativos. A través de ellos, se puede visualizar vulnerabilidades como latencia y congestión que puedan afectar a los equipos, puertos y conexiones.**

## 

## **Herramientas para el análisis de redes**

Estas herramientas no son las indicadas para resolver los mayores problemas en tus redes, pero sí **pueden otorgarte información importante** para que puedas ocuparte y realizar un mejor desempeño.

### **1. Nmap**

Cualquier especialista en sistema ha trabajado en algún momento con esta herramienta, generalmente, es utilizada en lo **referente a la seguridad informática y para la realización de pruebas de penetración.**

También, es muy común que se utilice para comprobar **si existen aplicaciones no autorizadas que estén valiéndose de las vulnerabilidades del sistema** para robar o compartir información de la red o de los sistemas. Los principales servicios que otorga esta herramienta son:

* **Descubre servidores**
* **Datos de hardware**
* **Servicios de ejecución**
* **Puertos abiertos**
* **Fingerprinting**

Como cualidad positiva, esta herramienta **no interfiere en el uso normal del sistema mientras está realizando sus funciones**, así no deben pararse las operaciones de la organización en medio del análisis. **Nmap** es compatible con sistemas operativos como Linux, Windows, Mac, entre otros.

Otro de sus puntos fuertes es que cuenta con una **interfaz gráfica** que facilita su uso y permite ver con mayor claridad el estado de la red y sus principales elementos.

### **2. NBTscan**

Esta herramienta sirve para **analizar puertos y te permite verificar si existe la utilización de recursos compartidos** de manera incorrecta. Por lo general, se basa en carpetas compartidas.

Este **escaneo de puertos** da mucha información referida a buscar recursos y muy simple de usar. Igualmente, es **compatible con los sistemas operativos Linux, Mac y Windows**, este último lo tiene integrado y puedes realizar el análisis directamente desde la computadora.

### **3. Netcat**

Se encarga de **interpretar los comandos y realizar rastreos de puertos**. Aunado a esto, permite el paso de archivos entre equipos porque abre los puertos y queda disponible para conectarse con un puerto de cualquier máquina que esté disponible. **A través de esta herramienta te será posible abrir conexiones TCP y UDP.**

Los administradores de sistemas la utilizan de forma cotidiana para la realización de depuraciones en los sistemas, igualmente es común que los hackers la aprovechen en las redes.

Todas estas herramientas son ampliamente conocidas en el mundo de la informática, **algunas más simples que otras y con una utilidad específica.**

Hay muchas otras que se pueden emplear, pero estas cuentan con un **interfaz simple** y realizan su trabajo de **manera fiable y rápida.** Lo importante es crear un diagnóstico a tiempo para mejorar las cualidades del sistema.