

Alumno: Rodrigo Vila

Modulo 2 Unidad 4 - Ejercicio adicional: Comandos de red de importancia (Windows)

"En esta unidad, solicita al instructor un documento para su lectura y comprensión, donde a través del mismo, podrán ponerse al tanto de los comandos de Windows, más utilizados en todo lo relacionado con troubleshooting de redes e investigación de datos de los entornos de red."

Te invitamos a que lo leas y que des tu opinión sobre el uso de los mismos respondiendo estas preguntas:

1- ¿Cuál piensan que es el objetivo principal de estos comandos?

- **IPConfig:** Muestra la configuración de red actual de un dispositivo, incluyendo su dirección IP, máscara de subred, puerta de enlace predeterminada y más.
- **Ping:** Envía un paquete de datos a un dispositivo o dirección IP específica para verificar si está alcanzable a través de la red. También proporciona información sobre la latencia (ping) entre los dispositivos.
- **ARP (Address Resolution Protocol):** Se utiliza para mapear direcciones IP a direcciones MAC en una red local. Ayuda a los dispositivos a determinar la dirección física de otro dispositivo en la misma red.
- **Tracert (o traceroute):** Muestra la ruta que toma un paquete de datos desde el origen hasta el destino, mostrando todos los saltos intermedios (routers) que atraviesa y el tiempo que tarda en cada uno.
- **Route:** Muestra y modifica la tabla de enrutamiento de un dispositivo. Esta tabla determina cómo se enrutan los paquetes de datos en una red, incluyendo qué interfaces y puertas de enlace se utilizan.
- **Netstat (Network Statistics):** Muestra estadísticas detalladas sobre las conexiones de red activas, tanto entrantes como salientes, así como información sobre los puertos utilizados y las tablas de enrutamiento.
- **NBTStat (NetBIOS over TCP/IP Statistics):** Proporciona información sobre las conexiones NetBIOS en un sistema que utiliza el protocolo TCP/IP. Puede mostrar estadísticas y resolución de nombres NetBIOS.
- **Nslookup (Name Server Lookup):** Utilizado para consultar servidores de nombres (DNS) para obtener información sobre nombres de dominio y direcciones IP asociadas.

Puede usarse para realizar búsquedas de direcciones IP, resolución inversa y otros tipos de consultas DNS.

2- ¿Si tuvieran la oportunidad de crear un nuevo comando de red, que te gustaría que haga?

Sería interesante tener un comando de red que pudiera realizar un análisis profundo de la seguridad de la red local. Algo así como lo que podemos lograr con la combinación de varias aplicaciones ya sean de Windows o Linux pero combinadas para el análisis integral de la seguridad de una red. Por ejemplo imagino un comando llamado "NetSecure" que pueda escanear todos los dispositivos en la red y detectar vulnerabilidades de seguridad, como puertos abiertos, configuraciones de firewall débiles, dispositivos con firmware desactualizado, contraseñas predeterminadas o débiles, y otras posibles brechas de seguridad. Además, podría ofrecer recomendaciones específicas para remediar estas vulnerabilidades, como cambiar contraseñas, actualizar firmware, cerrar puertos no utilizados, etc. Este comando sería útil para administradores de red y usuarios domésticos por igual, ayudándoles a mantener sus redes seguras y protegidas contra amenazas.

Algo así como un "Nmap" con esteroides. Ejecutado desde una terminal con permisos totales sobre los demás dispositivos pero a nivel de red, que permita escritura, modificación, lectura, etc. de configuraciones de red y más. Una especie de control total sobre la red. Aunque sería una herramienta tanto práctica como peligrosa, sería algo interesante.

Rodrigo Vila.-