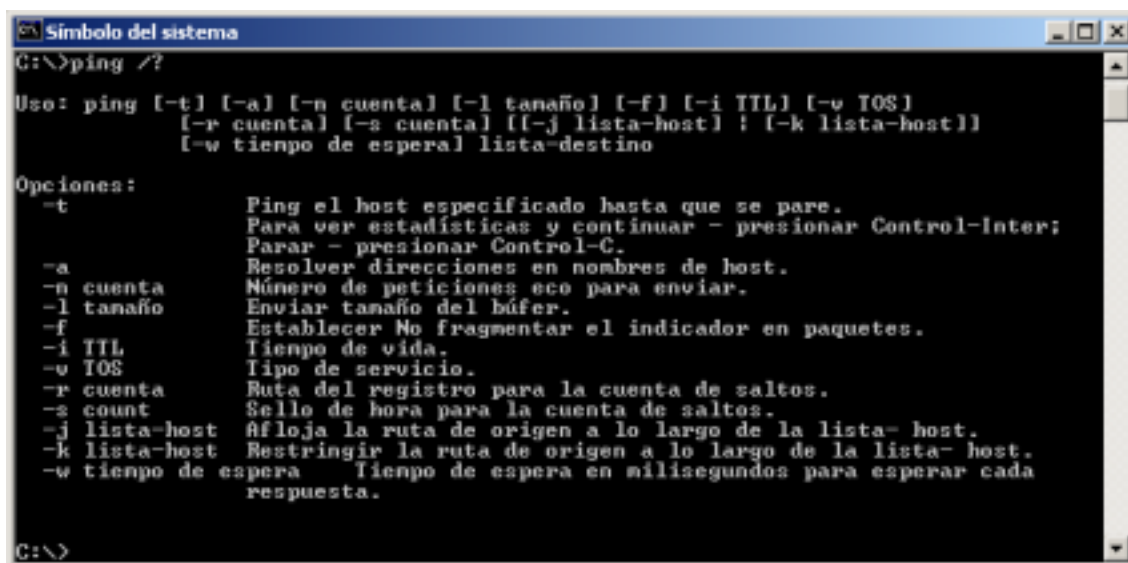


Práctica: 25. Barridos Ping y trazado de rutas (Por HxC Mods-Adm)

Para conocer si el/los equipos que buscamos están o no activos en la Red podremos utilizar la orden ping del Sistema operativo:



```
Simbolo del sistema
C:\>ping /?

Uso: ping [-t] [-a] [-n cuenta] [-l tamaño] [-f] [-i TTL] [-v IOS]
        [-r cuenta] [-s cuenta] [-j lista-host] [-k lista-host]
        [-w tiempo de espera lista-destino]

Opciones:
-t          Ping el host especificado hasta que se pare.
            Para ver estadísticas y continuar - presionar Control-Inter;
            Parar - presionar Control-C.
-a          Resolver direcciones en nombres de host.
-n cuenta  Número de peticiones: eco para enviar.
-l tamaño  Enviar tamaño del búfer.
-f          Establecer No fragmentar el indicador en paquetes.
-i TTL     Tiempo de vida.
-v IOS     Tipo de servicio.
-r cuenta  Ruta del registro para la cuenta de saltos.
-s count   Sello de hora para la cuenta de saltos.
-j lista-host Afloja la ruta de origen a lo largo de la lista- host.
-k lista-host Restringir la ruta de origen a lo largo de la lista- host.
-w tiempo de espera Tiempo de espera en milisegundos para esperar cada
            respuesta.
```

Basta con que indiques la dirección IP de la máquina o la dirección Web y la orden ping responderá afirmativa o negativamente de la existencia o disponibilidad del equipo remoto.

Muchos routers y firewall hoy en día rechazan sistemáticamente los ping entrantes, esto es debido a determinadas políticas de seguridad, de hecho hace algún tiempo era posible “tirar” un sistema con un simple ping, como ves en la sintaxis de la pantalla anterior es posible indicar el número de veces que se repite ping (-t para infinitos) e incluso el tamaño de los paquetes a enviar, un ping mal formado puede “despistar” al servidor, si además le añadimos miles de usuarios haciendo lo mismo un simple ping puede convertirse en un ataque DoS.

Para equipos con W95 y W98 es perfectamente “hacerles caer” con un ping -t -l 65500 ip.del.equipo, aunque no se consiga la caída del sistema realmentizaremos significativamente la conexión de la red.

Si deseas que tu equipo no responda a peticiones ping hay que filtrar el protocolo ICMP eco 17 y denegar y los puertos 135-139 y 445 de TCP/UDP para que no estén nunca visibles desde Internet.

Otro método para “desactivar” la respuesta a ping es usar filtros IPSec, el único inconveniente es que los filtros IPSec no pueden especificar específicamente a qué servicio ICMP debe rechazar, es decir, IPSec bloquea o permite todo el tráfico ICMP y además afectará a TODOS los adaptadores de red por igual.

Algunos IDS por software también son capaces de filtrar los barridos ping y de escaneo de puertos.

Muchas de las herramientas que estudiaremos en posteriores capítulos incluyen un barrido ping previo, no obstante y debido a las restricciones comentadas anteriormente que se aplican a nivel de router o cortafuegos, que un equipo no responda a un ping no significa que no esté disponible, por lo que actualmente ping es usado a nivel de la Intranet.

Otra herramienta para la localización de equipos es tracert, que además nos muestra los “saltos” que realiza la petición desde el equipo local hasta el equipo remoto. Tracert nos informará de las direcciones IP por las que va pasando el tráfico y el tiempo en milisegundos que tarda en conseguir la conexión.

Al igual que ping, también los routers y cortafuegos rechazan los trazados de rutas.