Ataques de reconocimiento

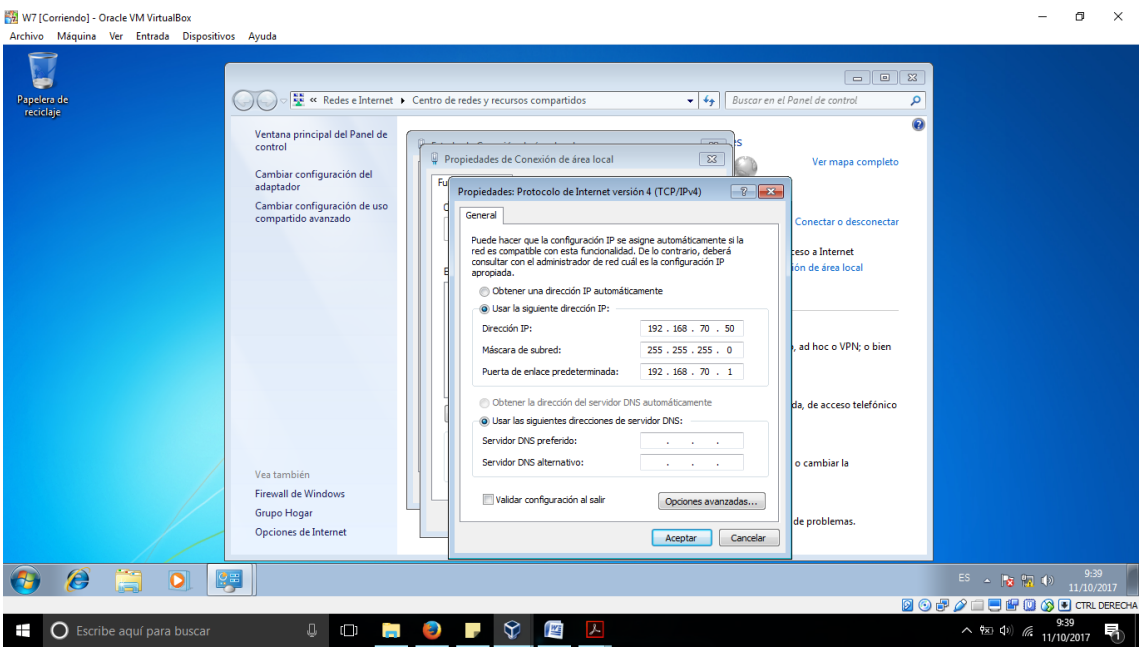
Un ataque de reconocimiento se refiere a la fase de preparación donde el atacante obtiene toda la información necesaria de su objetivo y/o víctima antes de lanzar un ataque. Es un método de administración de red que encuentra el rango de direcciones está en uso en la red.

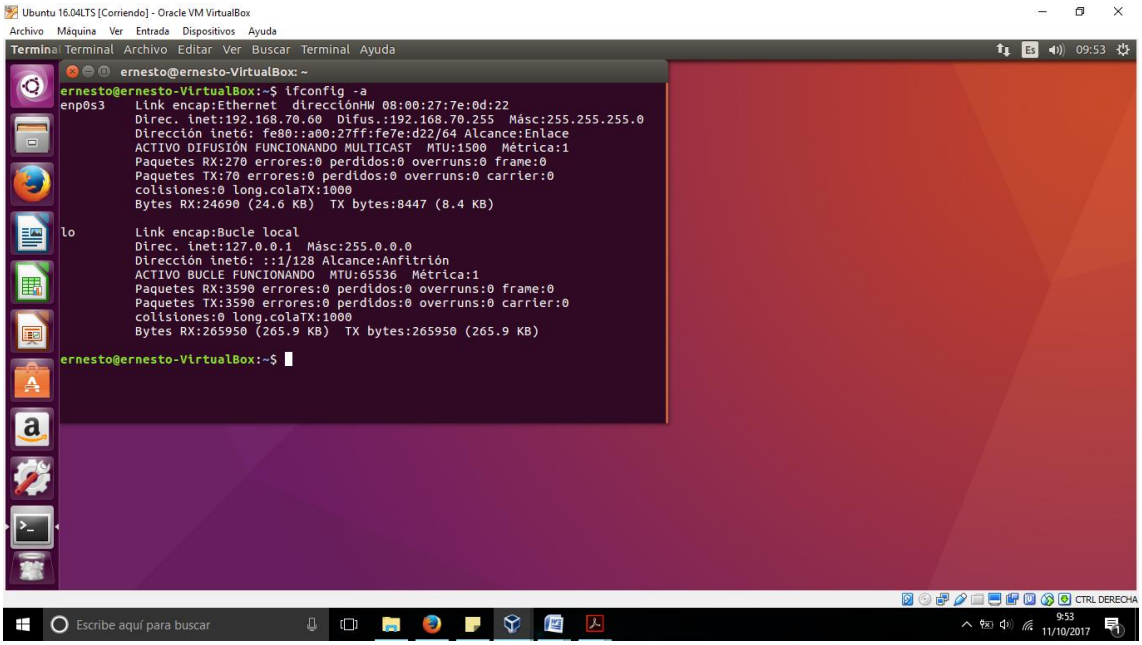
Los atacantes externos pueden utilizar herramientas de Internet, como las utilidades nslookup y whois, para determinar fácilmente el espacio de direcciones IP asignado a una empresa o a una entidad determinada. Una vez que se determina el espacio de direcciones IP, un atacante puede hacer ping a las direcciones IP públicamente disponibles para identificar las direcciones que están activas. Para contribuir a la automatización de este paso, un atacante puede utilizar una herramienta de barrido de ping, como fping o gping, que hace ping sistemáticamente a todas las direcciones de red en un rango o una subred determinados. Esto es similar a revisar una sección de una guía telefónica y llamar a cada número para ver quién atiende.

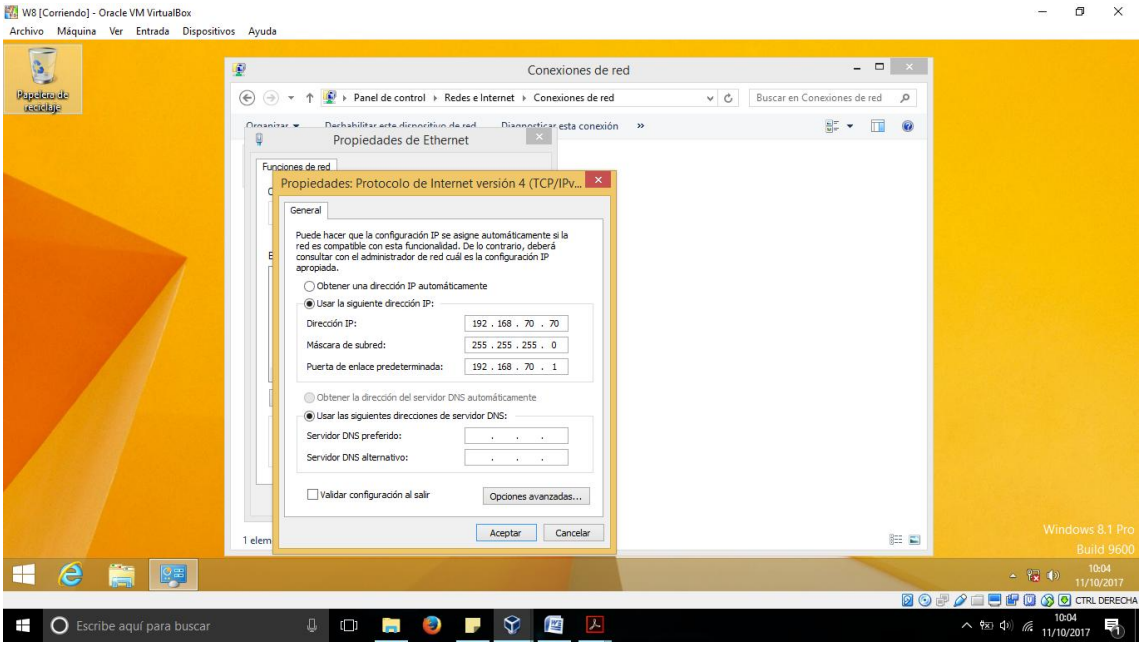
Para la práctica voy a usar los siguientes sistemas operativos:

- PC1- W7 que será el atacante.
- PC2- Ubuntu 16.04
- PC3- W8

Hay que configurar las tarjetas de red de los 3 sistemas con una IP estática y ponerlos en red interna.

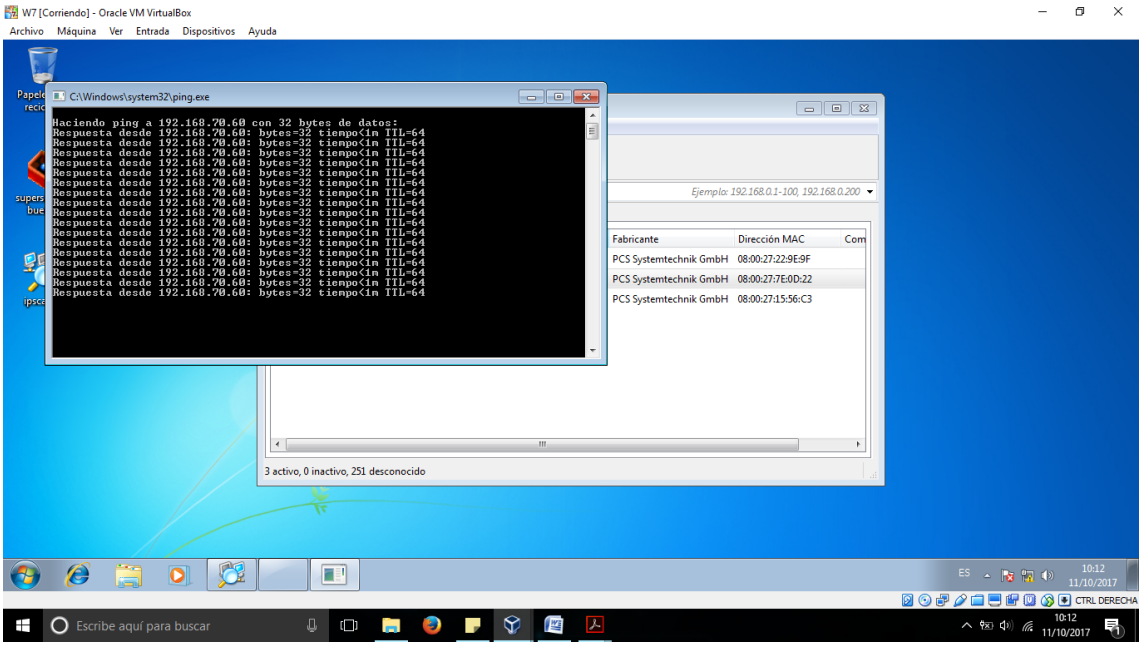






Utilizo el programa IP scan para hacer un barrido de pings a los equipos de la red interna.

Del PC1 al PC2

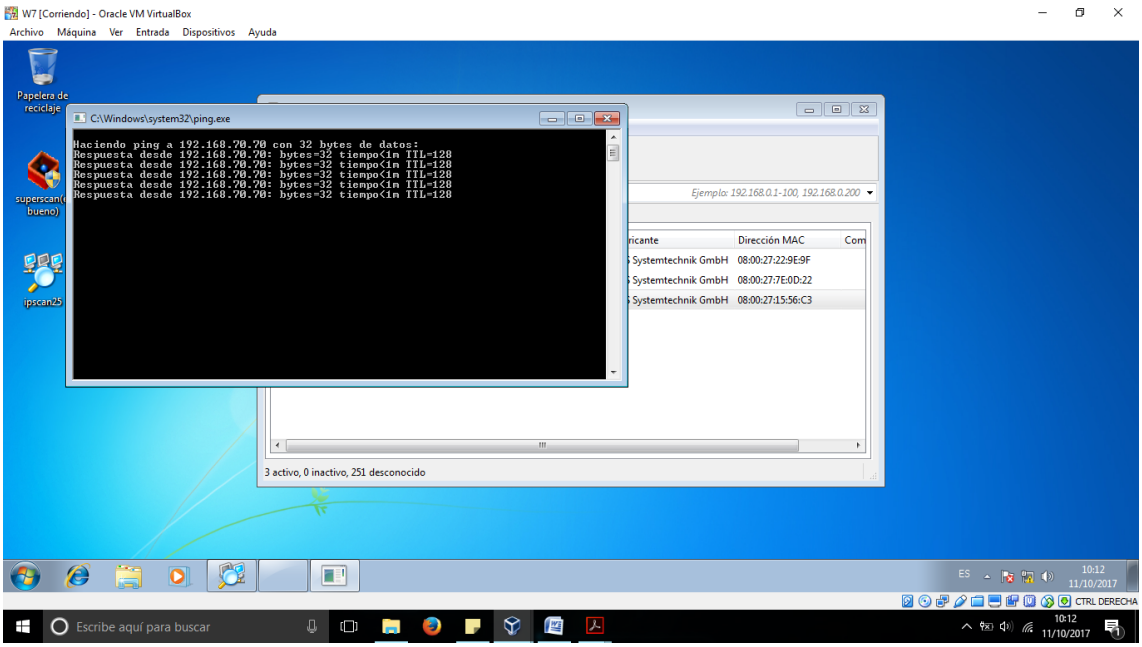


```
Haciendo ping a 192.168.70.60 con 32 bytes de datos:
Respuesta desde 192.168.70.60: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.70.60: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.70.60: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.70.60: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.70.60: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.70.60: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.70.60: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.70.60: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.70.60: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.70.60: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.70.60: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.70.60: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.70.60: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.70.60: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.70.60: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.70.60: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.70.60: bytes=32 tiempo<1m TTL=64
```

Fabricante	Dirección MAC	Com
PCS Systemtechnik GmbH	08:00:27:22:9E:9F	
PCS Systemtechnik GmbH	08:00:27:7E:0D:22	
PCS Systemtechnik GmbH	08:00:27:15:56:C3	

3 activo, 0 inactivo, 251 desconocido

Del PC1 al PC3

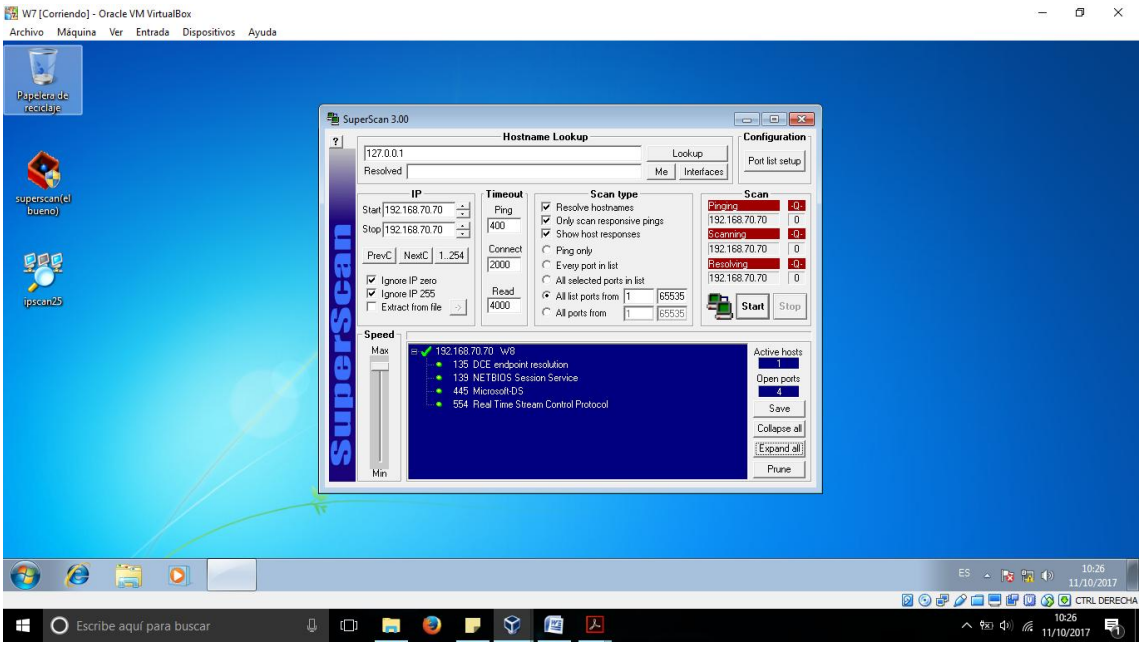


```
Haciendo ping a 192.168.70.70 con 32 bytes de datos:
Respuesta desde 192.168.70.70: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.70.70: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.70.70: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.70.70: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.70.70: bytes=32 tiempo<1m TTL=128
```

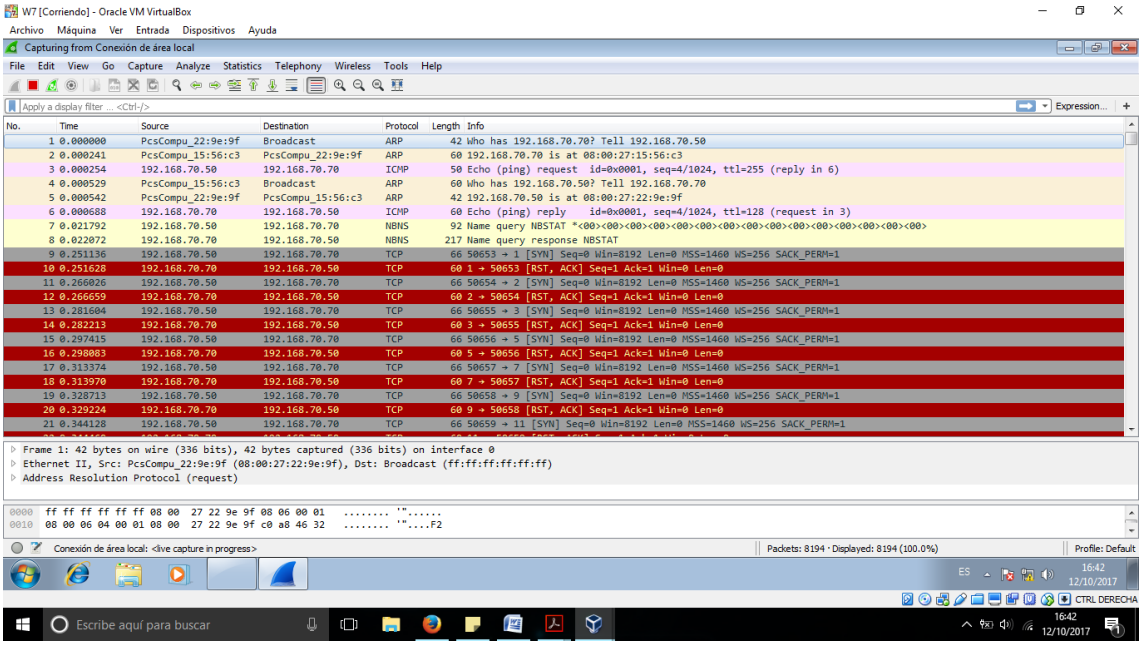
ricante	Dirección MAC	Com
Systemtechnik GmbH	08:00:27:22:9E:9F	
Systemtechnik GmbH	08:00:27:7E:0D:22	
Systemtechnik GmbH	08:00:27:15:56:C3	

3 activo, 0 inactivo, 251 desconocido

Con el programa SuperScan vamos a mirar los puertos que tiene abiertos el PC3, que va a ser el que reciba el ataque. Vemos que tiene 4 puertos abiertos.



Una vez escaneado usaremos Wireshark para capturar paquetes:



Software anti-sniffers

Un sniffer (también conocido como analizador de redes, analizador de paquetes o analizador de protocolo) es un programa de ordenador usado para controlar y analizar el tráfico red transmitido de una localización de red a otra. Un sniffer captura cada paquete de información, lo codifica y luego da a su propietario la habilidad de ver su contenido. Si un sniffer es usado por una persona respetable, no está considerado como una aplicación peligrosa, ya que es usado para generar información de errores y con propósitos de monitorización, o para detectar también intentos de intrusión en la red. Sin embargo, los sniffers pueden también ser usados por personas maliciosas que buscan robar información sensible de la gente transmitida a través de la red. Esta información puede ser muy diferente. Puede incluir datos de identificación de la víctima, contraseñas, detalles de la cuenta bancaria, números de tarjetas de crédito, detalles de identidad y otros datos valiosos que pueden ser usados para actividades peligrosas.

Actividad de un sniffer en el sistema y sus consecuencias:

Un sniffer no busca infectar el sistema con otras amenazas. Tampoco puede causar ningún problema en el rendimiento o estabilidad, ni simbolizar peligro alguno para los datos que están almacenados en tu ordenador. No obstante, una versión maliciosa de un sniffer puede fácilmente causar problemas relacionados con la privacidad. Este programa no necesita muchos recursos del sistema y no tiene una interfaz gráfica de usuario (GUI), por lo que es muy complicado detectarlo cuando está dentro de un ordenador. Una vez dentro, puede ser usado por hackers para violar la privacidad de la víctima. El control sin su consentimiento puede ser llevado a cabo durante meses e incluso años hasta que la víctima se de cuenta. Durante todo este tiempo, un sniffer es usado para proporcionar al atacante toda la información que necesite. Será capaz de localizar contraseñas, nombres de identificación, contactos, datos de identidad, incluso números de la tarjeta de crédito y mucho más. Toda esta información puede ser usada para entrar en el sistema, robar o mostrar datos confidenciales del usuario.

Éstas son las actividades más importantes necesarias para los desarrolladores de sniffers para alcanzar sus objetivos:

- Controlar el uso de red del usuario y filtrar paquetes definidos.
- Capturar todos los paquetes de red transmitidos de una localización de red a otra.
- Datos de identificación encontrados en paquetes capturados y guardarlos en un archivo.
- Dejar que el atacante analice los datos de identificación para conocer nombres, contraseñas, números de tarjeta de crédito, detalles identitarios u otra información valiosa.

Métodos usados para infiltrarse en los ordenadores:

Los sniffers no son virus y, por ello, no pueden propagarse a sí mismo y deben ser controlados por ciertas personas. Pueden ser instalados como cualquier otro programa con o sin el consentimiento del usuario. Hay dos métodos principales en los que los sniffers no solicitados pueden entrar en el sistema.

- Un sniffer puede ser manualmente instalado por el administrador del sistema o cualquier usuario que tenga suficientes privilegios para instalar el programa. Un hacker puede entrar en el sistema y configurar su propio sniffer malicioso. En ambos casos, la amenaza de privacidad se instala sin que el usuario afectado tenga conocimiento, ni mucho menos de su consentimiento.
- Los sniffers maliciosos se instalan a menudo por otros parásitos, como virus, troyanos, backdoors o gusanos. Éstos entran en el sistema sin el conocimiento del usuario y afectan a cada persona que use el ordenador comprometido. Estos sniffers no tienen ninguna función de desinstalación y pueden ser controlados solo por sus autores o por los atacantes.

Se recomiendan diferentes formas para rastrear “sniffers” dentro de nuestra red, he seleccionado algunos ejemplos al azar, para ayudar a los usuarios a rastrear la presencia de estas aplicaciones maliciosas que esperan pacientes.

<u>El Test del Ping</u>

Asumimos la opción –en este caso- de construir una petición tipo “ICMP echo” con la dirección IP del equipo sospechoso de hospedar un sniffer, pero con una dirección MAC deliberadamente errónea. Enviamos un paquete “ICMP echo” a nuestro objetivo con la dirección IP correcta, pero con una dirección de hardware de destino desigual.

Normalmente los sistemas denegarán este paquete, ya que su dirección MAC es incorrecta. No obstante, ciertos sistemas Linux, NetBSD y NT, puesto que el NIC está en modo heterogéneo, el sniffer tomará este paquete de la red como un paquete legítimo y responderá por relación.

Si el objetivo que analizamos reconoce a nuestra petición, tendremos claro que se encuentra en modo promiscuo. Un cibercriminal avanzado puede actualizar sus sniffers para filtrar tales paquetes, y hacer que parezca que el NIC no está en modo promiscuo.

<u>El test ARP</u>

Expedimos una petición ARP a nuestro objetivo con toda la información rápida excepto con una dirección hardware de destino errónea. Una máquina que no está en modo promiscuo nunca detectará dicho paquete. Si un equipo se encuentra en modo promiscuo, la petición ARP será atendida y el núcleo la procesará y contestará. El equipo que contesta queda en evidencia de que se encuentra en modo promiscuo.

Sniffers, ¿cómo nos protegemos?

En líneas generales para prevenir la acción de los sniffers y evitar que éstos alcancen sus objetivos de husmear contraseñas o en su defecto que nos “lean datos sensibles” en texto plano -sin cifrado fuerte-, podemos activar ciertas técnicas o recurrir a sistemas como:

- PGP
- SSL
- SSH
- VPN