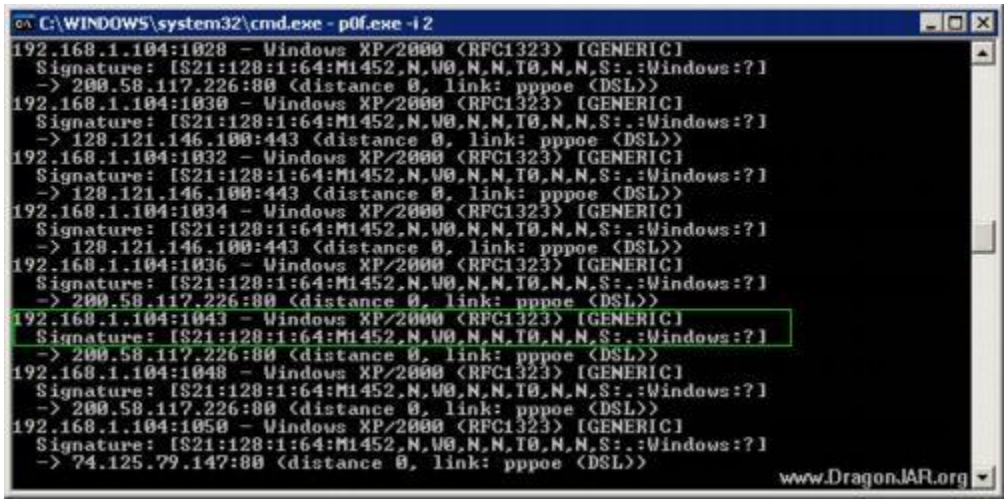
p0f – Identificación pasiva del Sistema Operativo

20. oct, 2008 8 Comentarios



P0f es una herramienta de identificación pasiva de sistema operativo, permite detectar el sistema y la versión de las maquinas conectadas a nuestro sistema, a las que nosotros nos conectamos, a las que podemos ver su trafico e incluso a las que no podemos conectarnos (bastante útil).

Aparte de todo esto P0f puede realizar otras tareas bastante interesantes, por ejemplo es capaz de dar una distancia física aproximada del sistema remoto, les dejo un pequeño listado de sus funciones “extra”:

- Detecta la existencia de un balanceador de carga.
- La distancia al sistema remoto y su tiempo en funcionamiento,
- Detecta la presencia de un firewall
- Identifica que conexión tiene el equipo remoto (DSL, OC3, avian carriers) y su proveedor de Internet.

El éxito de P0f es que no genera ningún trafico en la red, gracias a esto es posible identificar el sistema de equipos que estén detrás de un cortafuegos donde nuestro escanner habitual no podría llegar, ademas es liviano, rápido y funciona en entornos windows y gnu linux.

Puede descargar p0f v2 para GNU Linux Aquí

Puede descargar p0f v2 para Windows Aquí