icmpsh o cómo abrir un shell inverso mediante ICMP

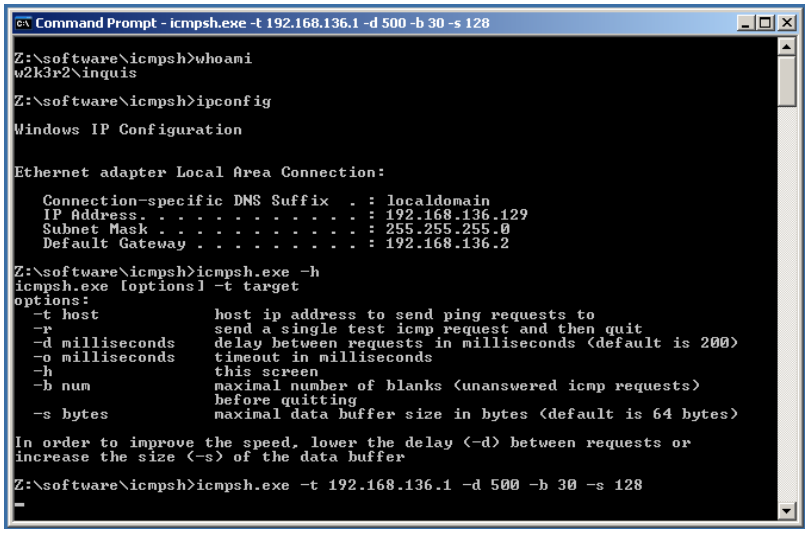
Publicado por Vicente Motos on lunes, 22 de octubre de 2012 Etiquetas: herramientas , técnicas

A veces los administradores de red nos ponen las cosas difíciles. Algunos de ellos, sorprendentemente, utilizan firewalls para lo que se supone que valen y obtener una shell inversa a través de TCP resulta difícil. No obstante, no es la primera empresa en la que me encuentro que **habilitan ICMP alegremente desde cualquier origen a cualquier destino**. Total, ¿qué podemos hacer con un simple ping?

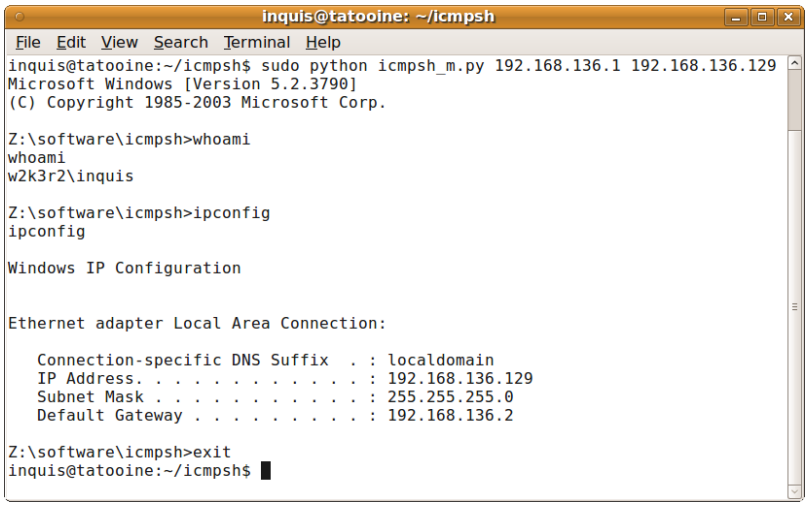
Pues, a parte de obtener información acerca de la topología de la red de los incautos administradores o estresar las tarjetas de red de alguna maquinita, podemos **establecer sesiones bajo nuestro amado protocolo**. Y no hace falta hablar en ruso o visualizar el código de Matrix, existen aplicaciones aptas para cualquier lammer que facilitan este trabajo como loki, soicmp o icmpshell y la herramienta de la que hablaremos en esta entrada: **icmpsh**.

¿Y por qué icmpsh y no otras? Pues porque es de código abierto y sobretodo **no requiere privilegios de administración** en la máquina objetivo. Es decir, la ejecutamos con nuestro usuario 'pelao' en un servidor comprometido (definido como slave) y ya tenemos una puerta abierta a través de cualquier firewall que se ponga por el medio. Eso sí, de momento el slave tiene que ser Windows, aunque **el master (o sea, nosotros los malos) puede ser cualquier plataforma que ejecute código C, Perl o Python**. Además, la herramienta de Nico Leidecker fue portada a Python por Bernardo Damele para poder integrarla en su famoso sqlmap (¿os suena, verdad?).

Para terminar, veamos un ejemplo ilustrado de su sencillo funcionamiento. Ejecutamos icmpsh slave en la máquina objetivo (192.168.136.129) especificando la IP 192.168.136.1 del master:



Y lanzamos icmpsh master en el equipo del atacante (192.168.136.1) y ejecutamos un par de comandos en la máquina comprometida (192.168.136.129):



Fuentes:

http://bernardodamele.blogspot.com.es/2011/04/reverse-connection-icmp-shell.html

https://github.com/inquisb/icmpsh

http://leidecker.info/downloads/index.shtml