**Hping3**

17 marzo 2017

Sergio Sánchez Basoco - A01339507

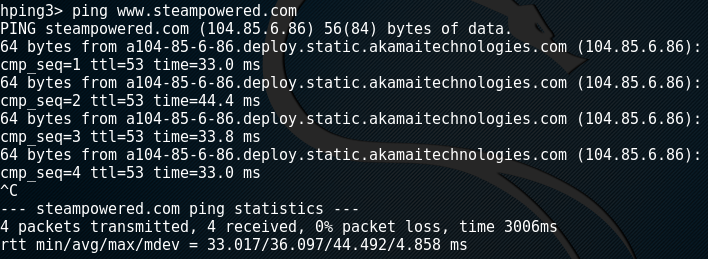
A01339507@itesm.mx

**1 Comandos básicos**

* 1. **Ping**

Para hacer un ping, simplemente deben introducirse los comandos siguientes:

(introducir hping3 en una línea antes para estar en modo hping3> como en la captura de pantalla)



Para terminar el proceso, presione CTRL+C y aparecerá finalmente alguna información adicional de transmisión de paquetes.

* 1. **Resolve**

El comando **resolve** nos permite saber la dirección IP de una URL en específico



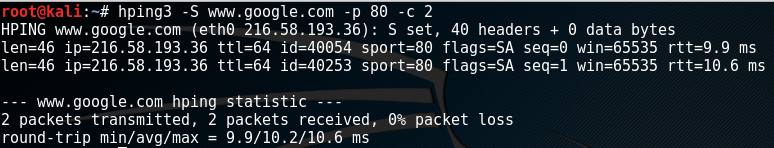
* 1. **Enviar paquetes**

Hping3 permite enviar paquetes TCP/IP, por ejemplo, para enviar un echo request ICMP se introducen los comandos siguientes:

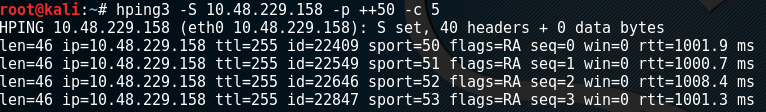


1. **Verificación de puertos**

Para checar un puerto en específico:

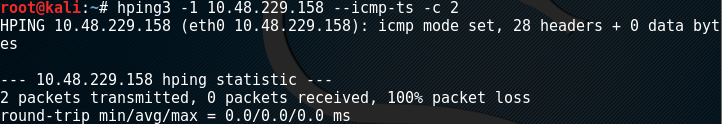


Para checar una serie de puertos:



“++” indica que este comando empezará por el puerto 50, si no asignamos un número específico de iteraciones “c”, el comando se va a ejecutar indefinidamente.

Debido a la flexibilidad que ofrece hping3 respecto a sus comandos, se pueden ejecutar comandos similares con gran diversidad de comandos, como:



Este comando nos permite saber si el host ha bloqueado ICMP, si hay respuesta quiere decir que ICMP no está boqueado.

hping3 -1 19

1. **Ataque DoS (*Denial of service)* simple**

Esta sección consiste en atacar un equipo mediante negación de servicio, se necesita una computadora con Windows y otra con Kali.

En Windows, obtenga la IP del equipo y abra Wireshark en donde deberá capturar los paquetes provenientes de la interfaz ethernet (asegurarse que el cable respectivo esté conectado a la computadora)

En Kali, ejecutar un ping a la computadora Windows, si es así, podemos proceder a introducir el comando para iniciar el ataque:

hping3 -c 100000 -d 120 -S -w 64 -p 21 --flood --rand-source 192.168.1.77

* -c 1000000 es el número de paquetes a enviar
* -d es el tamaño de cada paquete que se enviará a la víctima.
* -S se enviarán paquetes SYN únicamente.
* -w 64 es el “*TCP window size”*
* -p 21 es el puerto de la víctima, (se usó 21 para FTP) y se puede utilizar cualquiera.
* --flood quiere decir que se enviarán paquetes lo más rápido posible ignorando las respuestas de estos paquetes.
* --rand-source quiere decir que los paquetes se enviarán utilizando direcciones IP aleatorias.
* 192.178.1.77 es la dirección de la víctima.

Lo esperado es que después de un par de minutos, en el administrador de tareas se observe un 90% de uso de memoria RAM, red y en ocasiones de disco/procesador.

Se podría incrementar la intensidad del ataque si se utilizan dos o más equipos con la misma función.