



**Ataques ICMP
contra TCP**

Fernando Gont
UTN/FRH, Argentina

Jornada de Seguridad en Internet
15 de agosto de 2007, Montevideo, Uruguay

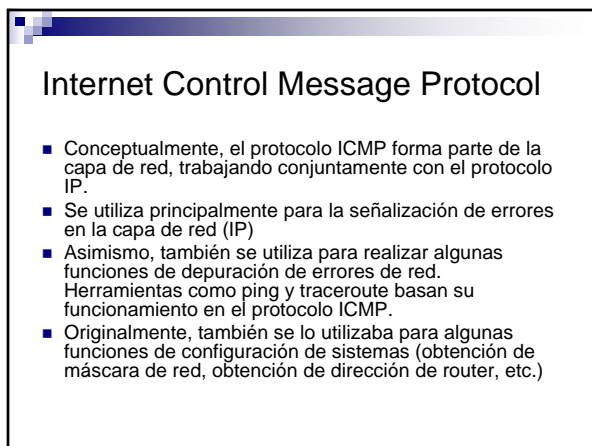




Aislamiento de fallas y recobro de fallas en la Arquitectura de Internet

Dos funciones básicas en una red de computadoras son el **aislamiento de fallas** y el **recobro de fallas**.

- El aislamiento de fallas consiste en detectar condiciones de error en la red (sistemas inalcanzables, etc.)
- El recobro de fallas consiste en intentar sobrevivir esas condiciones de error.
- La Arquitectura de Internet delega la función de aislamiento de fallas al protocolo ICMP.



Internet Control Message Protocol

- Conceptualmente, el protocolo ICMP forma parte de la capa de red, trabajando conjuntamente con el protocolo IP.
- Se utiliza principalmente para la señalización de errores en la capa de red (IP)
- Asimismo, también se utiliza para realizar algunas funciones de depuración de errores de red. Herramientas como ping y traceroute basan su funcionamiento en el protocolo ICMP.
- Originalmente, también se lo utilizaba para algunas funciones de configuración de sistemas (obtención de máscara de red, obtención de dirección de router, etc.)

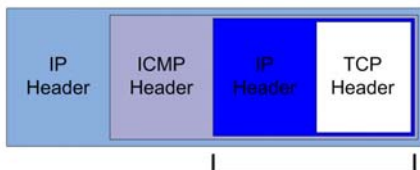
Demultiplexación de mensajes ICMP

- Cuando un sistema recibe un mensaje ICMP, se desea notificar dicho evento a la instancia de comunicación que lo produjo, con el fin de que el correspondiente protocolo de transporte realice su operación de "recobro de fallos".
- Con el fin de posibilitar esta operación, los mensajes de error ICMP incluirán una porción del paquete que causó el error en cuestión, bajo la suposición que dicha porción del paquete original proveerá toda la información necesaria para demultiplexar el mensaje de error.
- Las especificaciones de la IETF requieren que se incluya en el mensaje de error ICMP al menos el encabezado IP completo y los primeros 8 bytes del payload del paquete que generó el mensaje de error.

Información incluida en los mensajes ICMP



Estructura del paquete resultante



El paquete ICMP contiene en su "payload" parte del paquete original que causó el error. Dicho paquete ICMP se encapsula en un paquete IP, para ser enviado hacia el sistema que debe recibir el mensaje de error.

Validación de mensajes ICMP

Las especificaciones de la IETF no recomiendan ningún tipo de chequeo en los mensajes de error ICMP recibidos.

Esto significa que siempre que el mensaje de error ICMP contenga los valores {source IP, source TCP port, destination IP, destination TCP port} correctos, será pasado a la correspondiente instancia de TCP, y será procesado, causando las acciones recomendadas por las especificaciones

Información necesaria para atacar

Para lograr que un mensaje de error ICMP sea entregado a una instancia de TCP dada, el atacante tendría que "adivinar":

- Dirección IP origen (Source IP)
- Dirección IP destino (Destination IP)
- Puerto TCP origen (Source TCP port)
- Puerto TCP destino (Destination TCP port)

En principio, esto haría suponer que la información necesaria para realizar ataques mediante la falsificación de mensajes ICMP es demasiada como para que los ataques sean realizables en la práctica.

Sin embargo, no hay tanto que adivinar....

- La dirección IP del servidor usualmente será conocida
- La dirección IP del cliente podría ser conocida
- El puerto TCP del servidor usualmente será conocido
- El puerto TCP del cliente usualmente no será conocido, pero podrá ser adivinado

Asumiendo que el atacante conoce las partes involucradas, y el servicio utilizado por las mismas,

Cuanto mucho, el atacante deberá enviar 65536 paquetes para realizar cualquier tipo de ataque ICMP contra TCP

Rango de puertos efimeros

La mayoría de los sistemas eligen sus "puertos efimeros" de un subespacio de todo el espacio de puertos disponible

Sistema operativo	Puertos efimeros
Microsoft Windows	1024 - 4999
Linux kernel 2.6	1024 - 4999
Solaris	32768 - 65535
AIX	32768 - 65535
FreeBSD	1024 - 5000
NetBSD	49152 - 65535
OpenBSD	1024 - 65535

Número práctico de paquetes requeridos para realizar un ataque ICMP contra TCP

En la mayoría de los casos, el atacante precisará enviar **a lo sumo 4K** paquetes para realizar cualquier ataque ICMP contra TCP

Con un enlace de 128 kbps, esto llevaría nada más que **unos pocos segundos!**

El eslabón mas débil de la cadena

- Ninguna de las contra-medidas existentes para proteger a TCP de otros ataques ayudan a proteger TCP de los ataques ICMP
- Los mensajes ICMP pueden provenir desde cualquier sistema de Internet. Es imposible predecir qué router encontrará una condición de error, por lo cual es imposible predecir qué sistema enviará un mensaje de error ICMP. Asimismo, un sistema podría tener más de una dirección IP, y enviar el mensaje de error ICMP utilizando cualquiera de ellas.
- Esto implica que no hace falta falsificar la dirección de origen de los mensajes ICMP, siquiera.

Todas estas consideraciones hacen que los ataques ICMP sean los mas simples de realizar contra TCP y otros protocolos de transporte similares
