

# TCP/ICMP TÚNEL



Undercon 8

laM

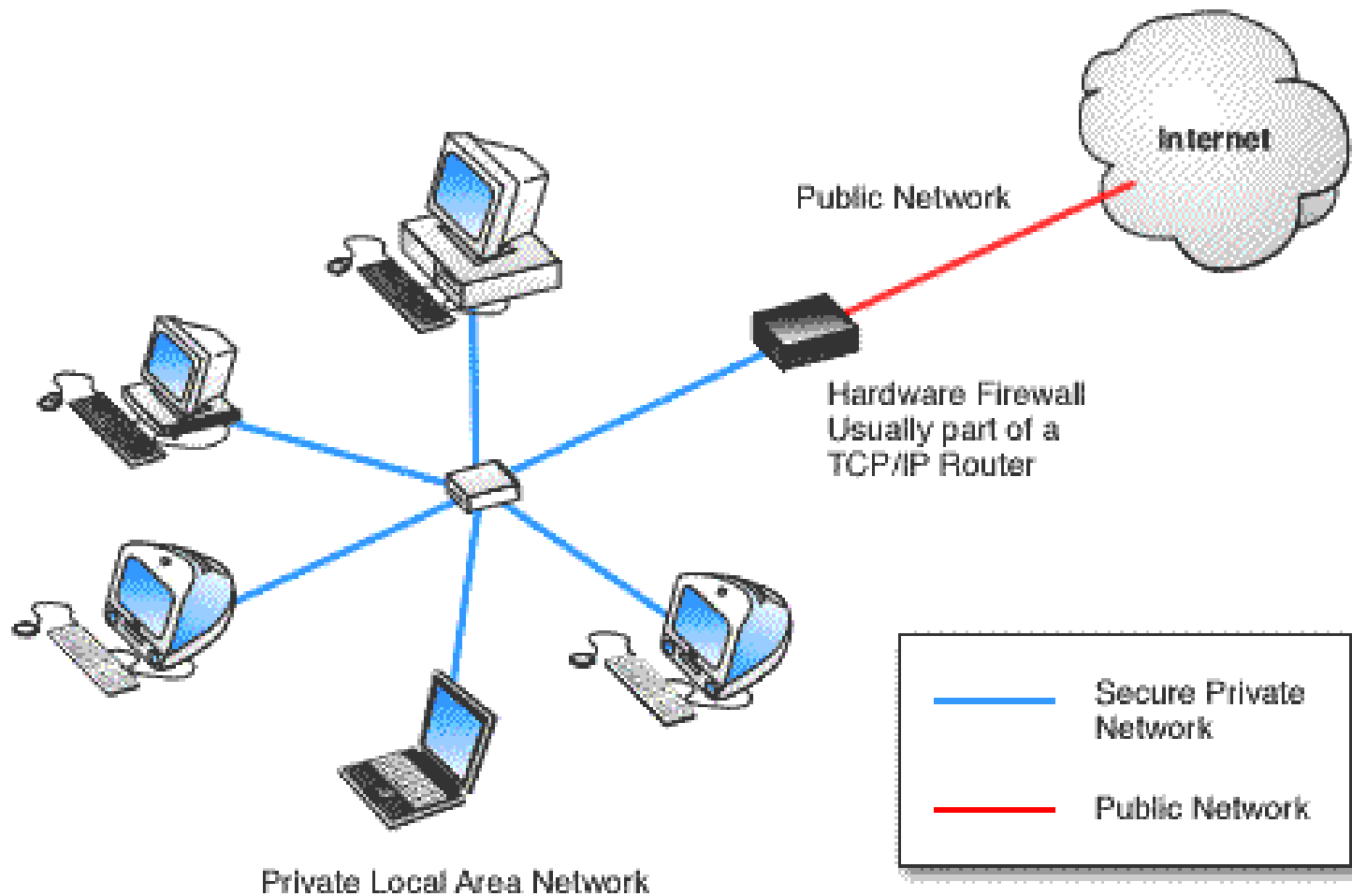
# Introducción

- En entornos de pentesting profesional, a menudo nos encontramos con firewalls que no filtran los paquetes ICMP de tipo TIMESTAMP.
- Banca, PYMES, ISPs...

# Introducción

- Estos firewalls, están correctamente configurados:
  - ✓ No permiten el paso del tráfico desde el exterior salvo en un puerto, normalmente el 80.
  - ✓ Tampoco permiten el paso del tráfico desde dentro hacia fuera.

# Escenario



# Una vez dentro...

- Nos hemos aprovechado de un cgi, vulnerabilidad común, etc.
- No podemos colocar una backdoor para trabajar **cómodamente**.
- Podemos llegar a root cambiando la shellcode o a veces no hace falta ni eso, por ejemplo con el bug del kernel de Solaris (entorno muy común en servidores de banca).
- Es difícil entrar mas adentro (estamos limitados, tanto en tiempo como en medios).

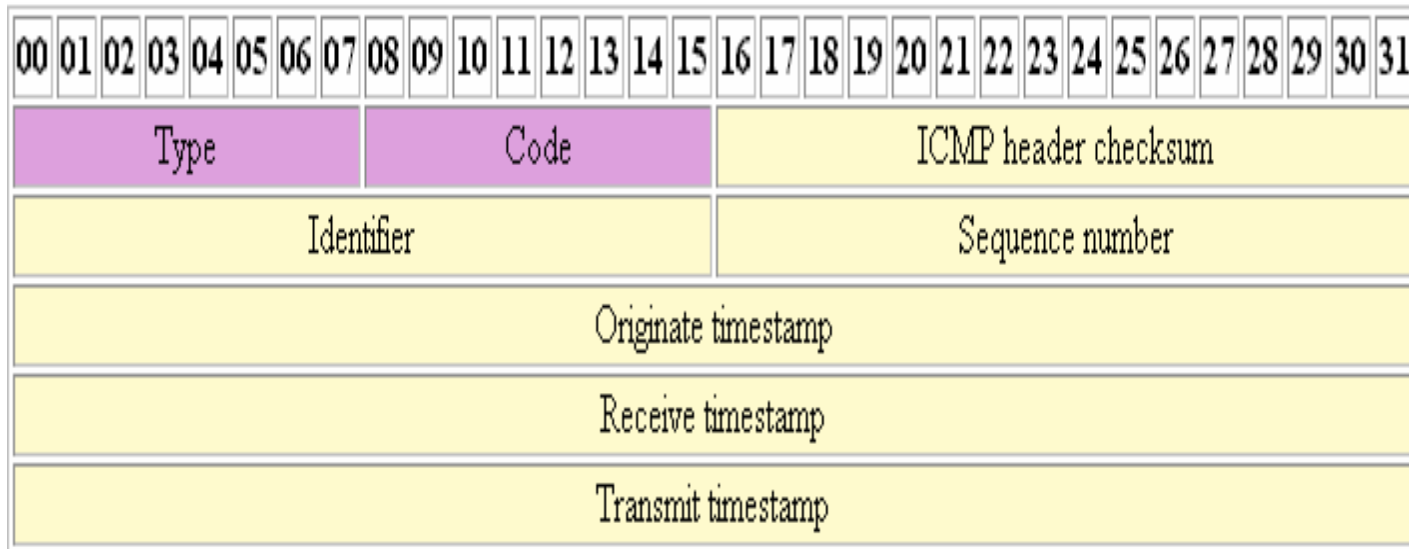
# Tenemos una posibilidad

- En los informes se presentan alertas del tipo: **Este host no tiene filtrado los paquetes ICMP de tipo timestamp.**
- Hay que desarrollar un tunel que nos permita pasar de trafico TCP a trafico ICMP timestamp y al revés.

# Problemas

- **EL ICMP TIMESTAMP:**
  - No tiene cabecera de datos.
  - No está orientado a conexión
  - Es el primer tipo de paquete que se descarta en una red saturada.
  - Llega con errores o en orden aleatorio.

# Esquema del paquete ICMP TIMESTAMP



# Soluciones

- Para enviar los datos podemos utilizar los  $32 \times 3 = 96$  bits de Originate, Receive y Transmit timestamp (12 bytes).
- Para enviar los datos de manera fiable, tenemos que diseñarnos nuestro propio protocolo.

# Protocolo de bit alternante

- Protocolo fiable de envío de datos.
- Utiliza dos tipos de tramas: envío y asentimiento:
  - Trama de datos: tipo, num secuencia, datos
  - Trama de asentimiento: tipo, num secuencia, datos

# Comportamiento

- Tramas de datos numeradas consecutivamente.
  - ✓La trama de asentimiento asiente con el número de secuencia de la próxima trama esperada.
- Numero de secuencia: Entero.
- Tamaño de la ventana: 1.
  - ✓Solo puede haber una trama por asentir.
- El emisor retransmite al cabo de 'X' segundos si no recibe asentimiento.
- En el campo Identifier se guarda el n<sup>o</sup> total de paquetes.

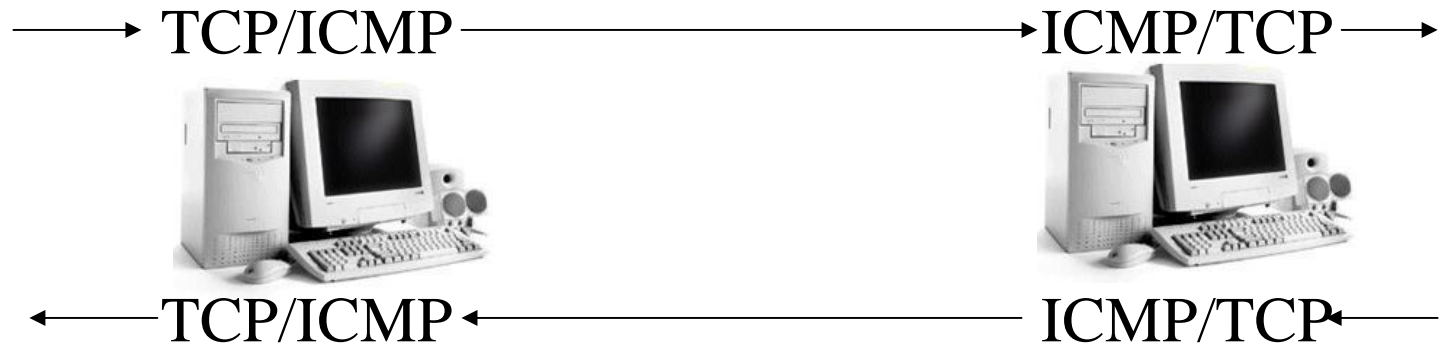
# Esquema resumido



# Esquema resumido

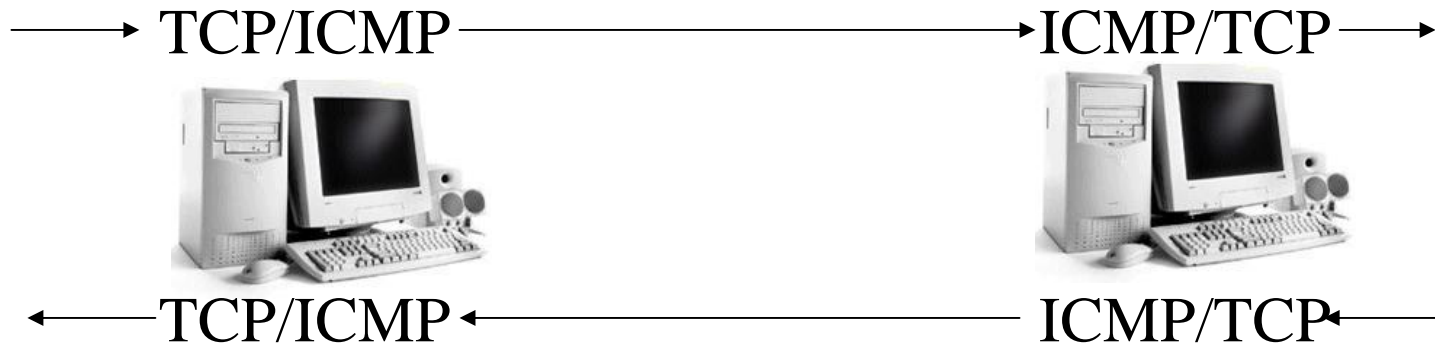


# Esquema resumido

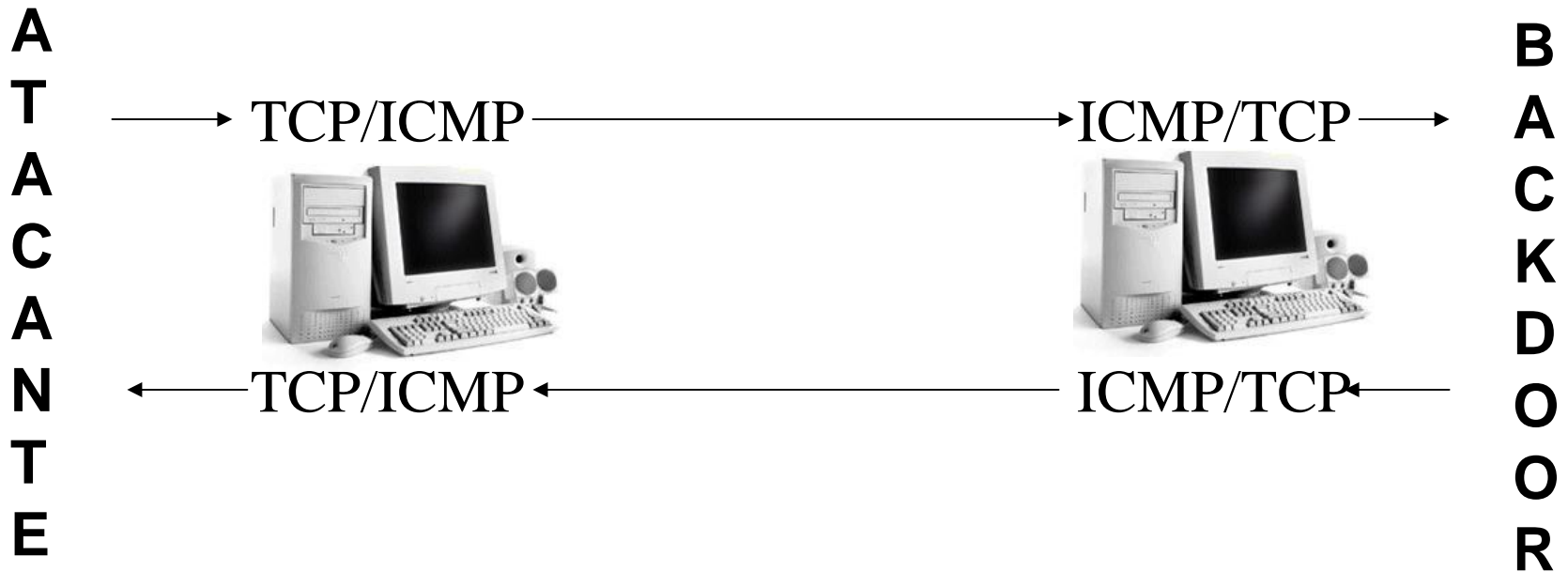


# Esquema resumido

A  
T  
A  
C  
A  
N  
T  
E



# Esquema resumido



# Utilidades

- Pasar Firewalls que permitan ICMP.
- Pasar sistemas de logueo wireless.
- No hace falta tener ningún puerto abierto.
- No hace falta modo promiscuo.
- Se ha programado la capa común para cualquier backdoor, el resto va a nuestro antojo: tsh, etc.
- Los datos van cifrados, y por tanto difíciles de detectar en los IDS.

¿Dudas?

**IaM – Murcia**

**<09/10/2004>**

**IaM@t0s.org**