Seguridad en Sistemas Informáticos

Intrusión 3: ataques a la red

Área de Ingeniería Telemática
Dpto. Automática y Computación
http://www.tlm.unavarra.es/

En clases anteriores...

- Búsqueda e Identificación de IPs
- Intrusión en sistemas

- Hoy
  - Ataques a la red

Network Hacking

- Ataques a la red y no a un host determinado
  - Ataque a la privacidad

    Quiero leer lo que circula por la red
  - Ataque al acceso

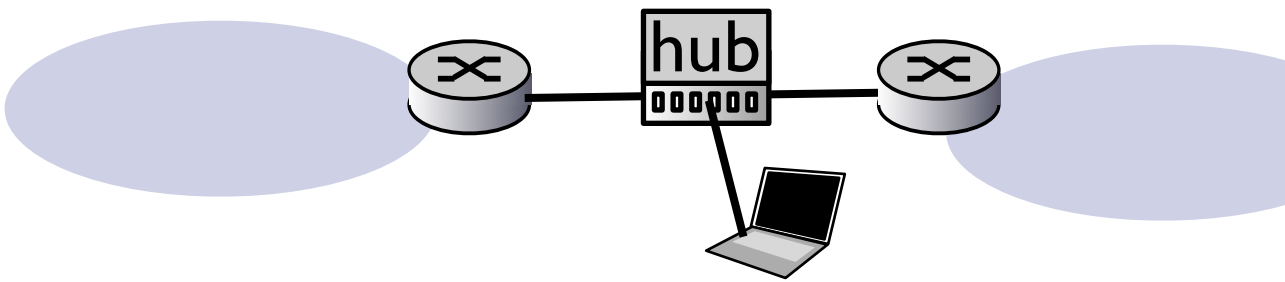
    Quiero usar los recursos de la red
  - Ataque de denegación de servicio

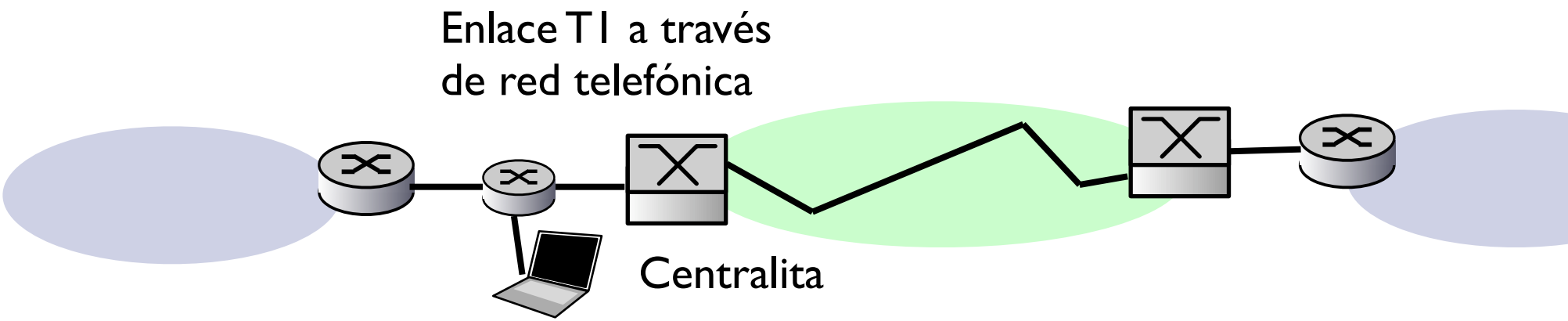
    Quiero que nadie use la red o el servidor X

- Siguiendo los niveles de la pila de protocolos

Network hacking: nivel 1 (físico)

- El nivel 1 puede ser interceptado (pinchado)
  - Fibra óptica, dificil
  - Cable Ethernet
  - Cable enlace T1





- Esto se llama ataque **Man-in-the-middle** (a nivel físico)
- En redes inalambricas es más fácil aun

Network hacking: nivel 2 enlace/LAN

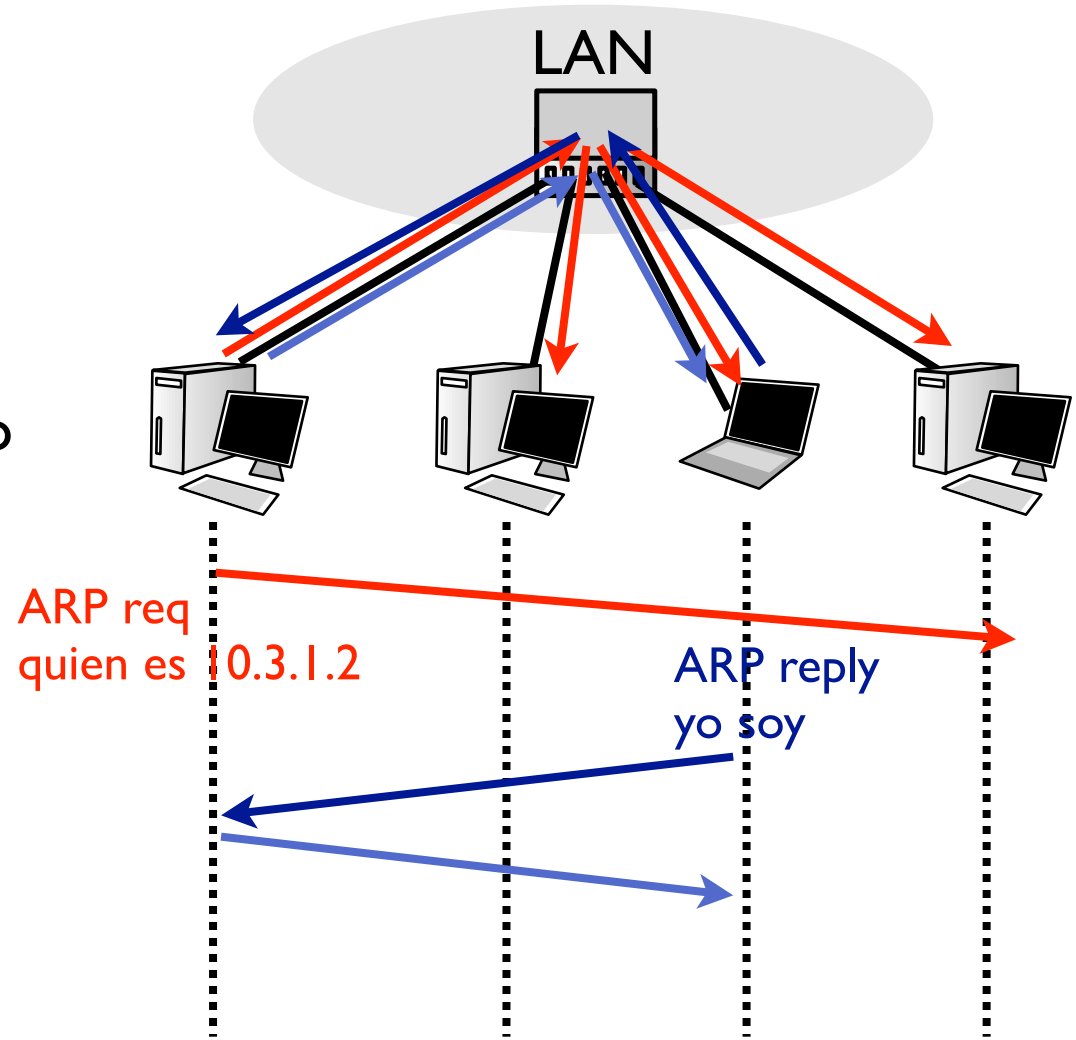
- Ethernet: medio compartido y resolución de colisiones
  - Cualquiera puede ver los paquetes que envían los demás
  - En una red formada por concentradores(hubs) es trivial espiar la red. (Herramientas: tcpdump, ethereal...)
- Recordando Redes de Computadores
  - Hubs ethernet: recibo todos los paquetes
  - Switch ethernet: solo paquetes dirigidos a mi
- Aparte de ser más eficiente (la capacidad se reparte mejor)

  es más seguro utilizar siempre conmutadores(switches) ethernet
  - Pero es suficiente???
  - ¿Que puede hacer un hacker si nuestra red esta formada por switches ethernet?

Network hacking: nivel 2 enlace/LAN

- Recuerde ARP
  - ARP request broadcast

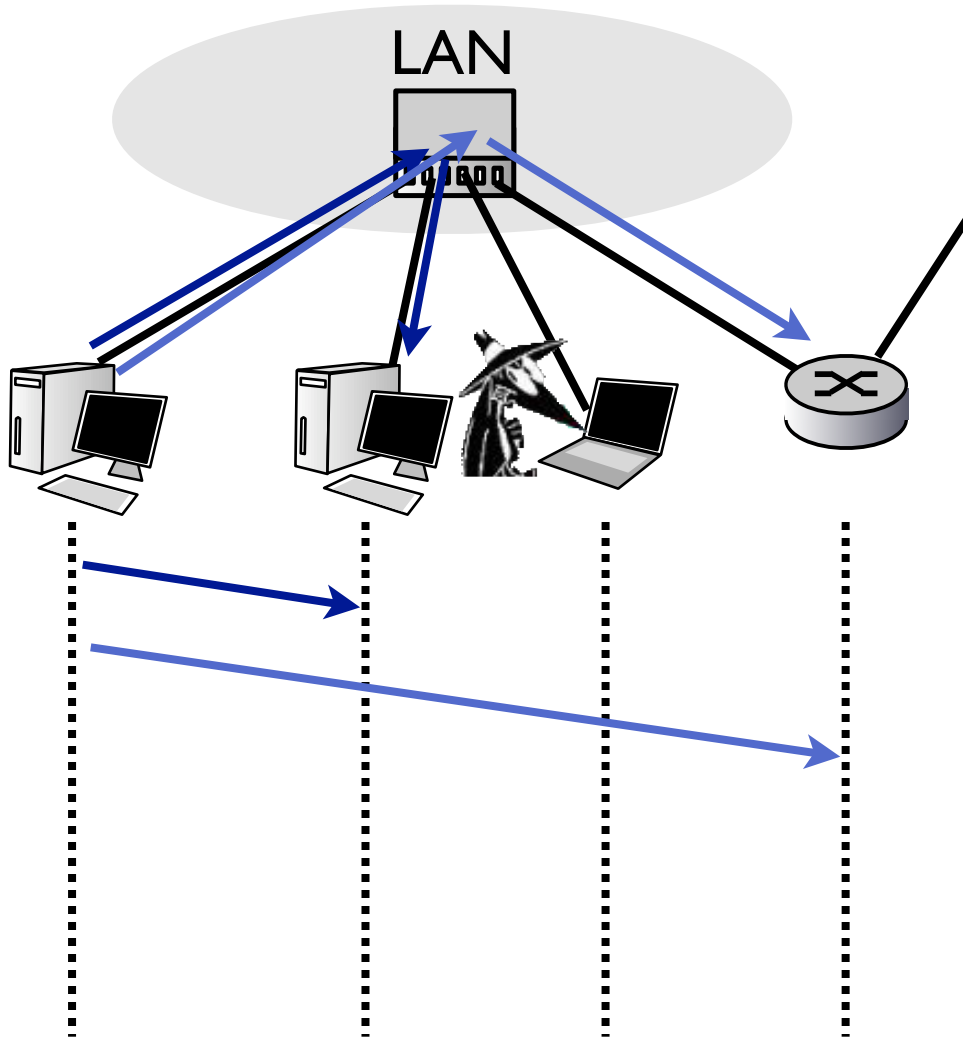
    quien tiene esta IP
  - El conmutador al ver pasar esta trama se aprende la MAC del emisor
  - ARP response dirigida al destino
  - El conmutador al ver pasar esta trama se aprende la MAC del emisor
  - Las tramas de A a C no pueden ser observadas por D



Network hacking: nivel 2 enlace/LAN

- En posteriores envios
- Los PCs tienen en cache la dirección MAC de sus destinos
- El conmutador ha aprendido en que puerto esta cada dirección MAC

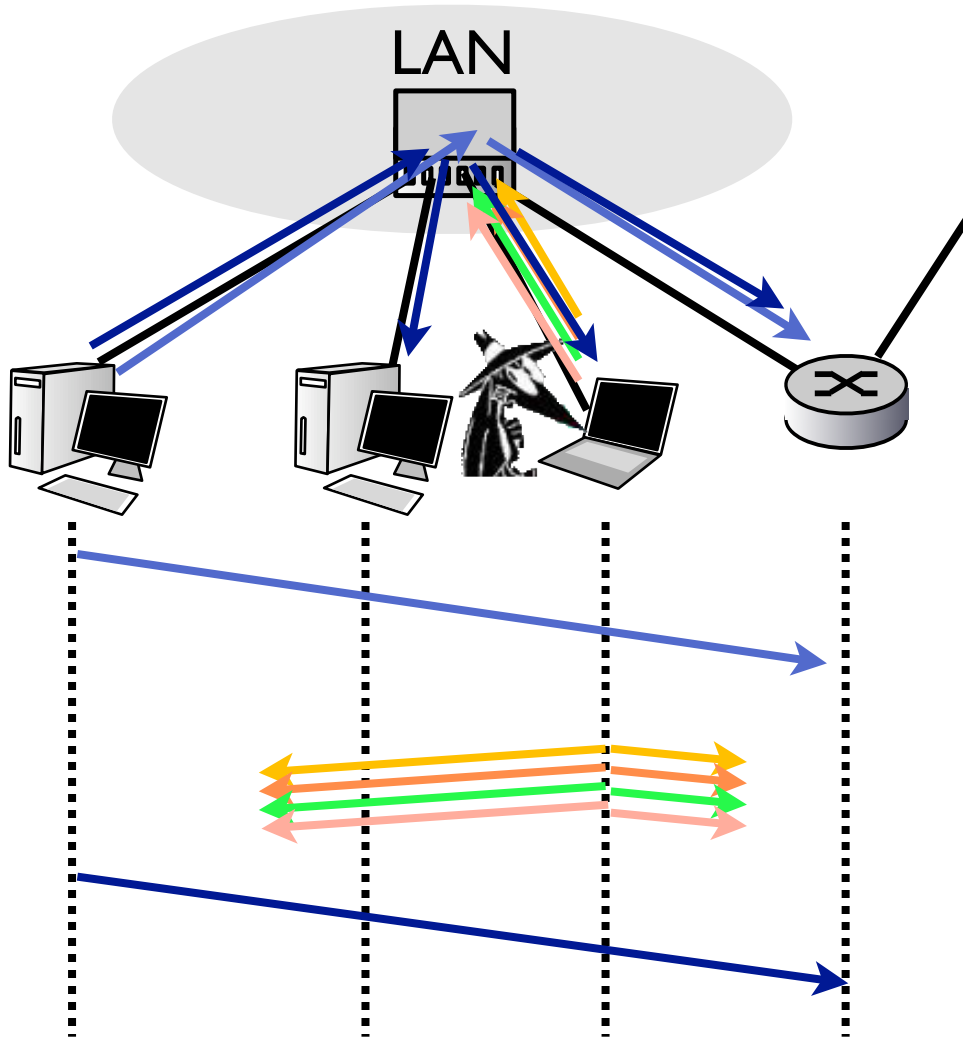
- Un hacker en un ordenador en el mismo conmutador no puede ver los paquetes entre A y B ni los que van al exterior



Network hacking: nivel 2 enlace/LAN

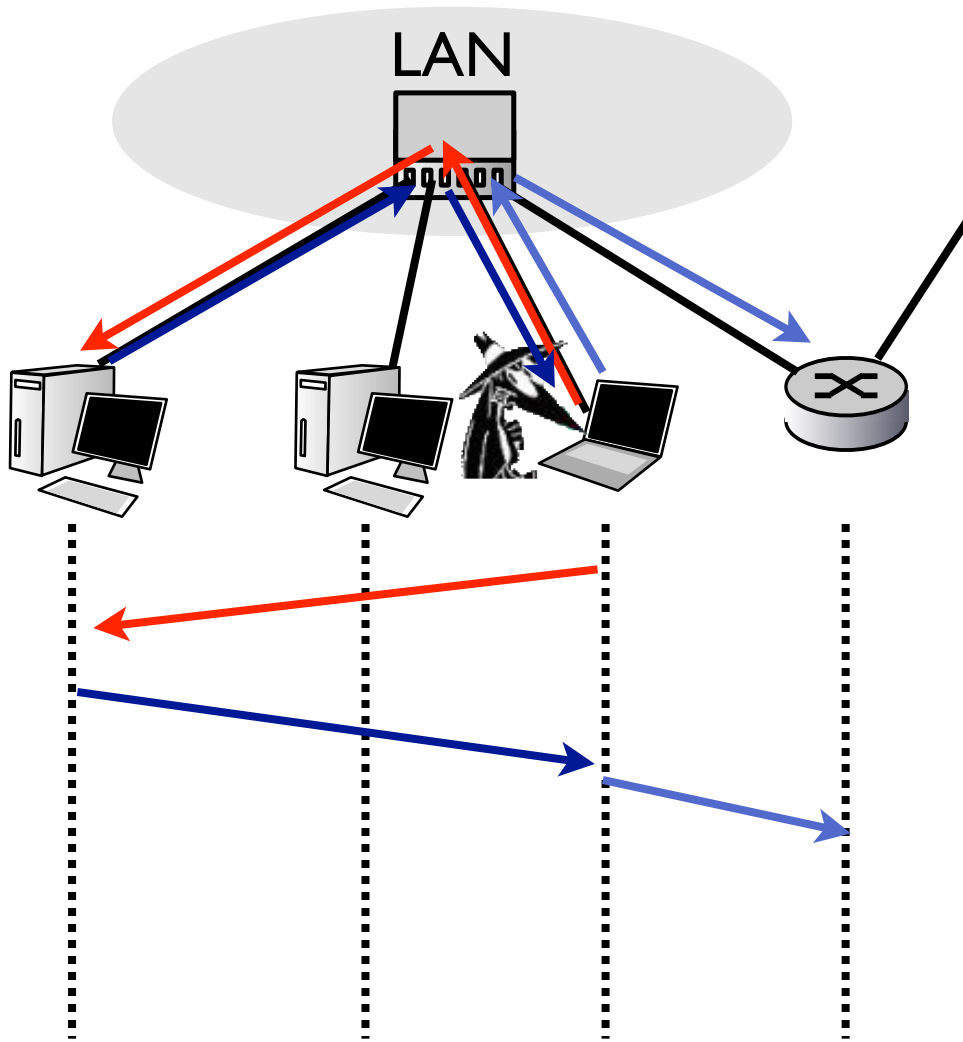
- Inundación con paquetes a direcciones MAC aleatorias

  (MAC spoofing)
- El conmutador se queda sin sitio en las tablas para apuntar donde estan las direcciones MAC
- Si no se donde esta una MAC la envío por todos los puertos
- Tenemos un switch que se comporta como hub
- Ya puedo usar un sniffer normalmente



Network hacking: nivel 2 enlace/LAN

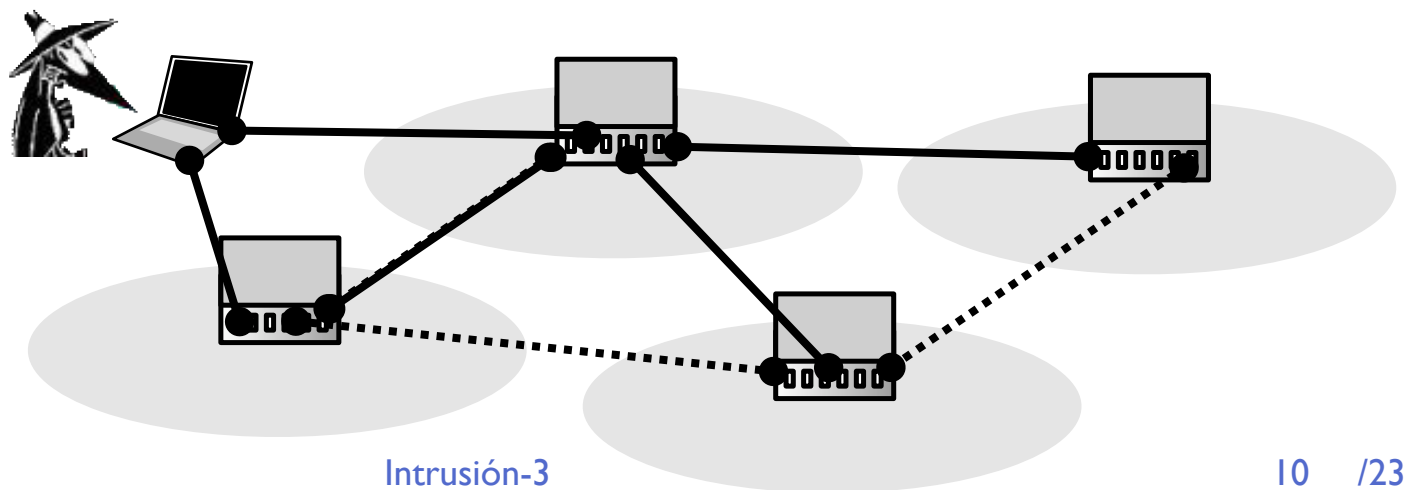
- Mejor todavía
  - El hacker activa IP forwarding (=router)
  - Envía un paquete ARP response a A diciendo que la IP del router esta en su MAC (arpredirect)
  - A modifica su cacheARP
- Cuando A tiene un paquete para enviar al exterior
  - Envía a la IP del router
  - La dirección MAC asociada a la IP del router es... la de C
  - El ordenador del hacker envía el paquete al router
- Man in the middle
- Se puede hacer en los dos sentidos



Network hacking: nivel 2 enlace/LAN

- **Redirección ARP (ARP redirection)** o

  Envenenamiento ARP (ARP poisoning)
  - También sirve como técnica de denegación de servicio enviando MACs falsas para interrumpir el trafico
  - Permite interceptar los datos en un conmutador entre destinos de los que se conoce la dirección MAC y observar el tráfico en un conmutador con un sniffer ethernet
  - Pero una vez que reenviamos los paquetes podemos también modificarlos
- **Sniffing broadcast**
  - Observando el tráfico broadcast también podemos sacar información (volúmenes exportados por Windows y AppleTalk...)
- **Ataques al STP**



Network hacking: nivel 2 enlace/LAN

- **Ataques a la asignación en niveles de enlace que necesitan establecimiento**
  - Ethernet no tiene
  - Niveles con establecimiento/asociación
    - WiFi
    - PPP
    - VPNs

- **Lo veremos en sesiones dedicadas a esto**

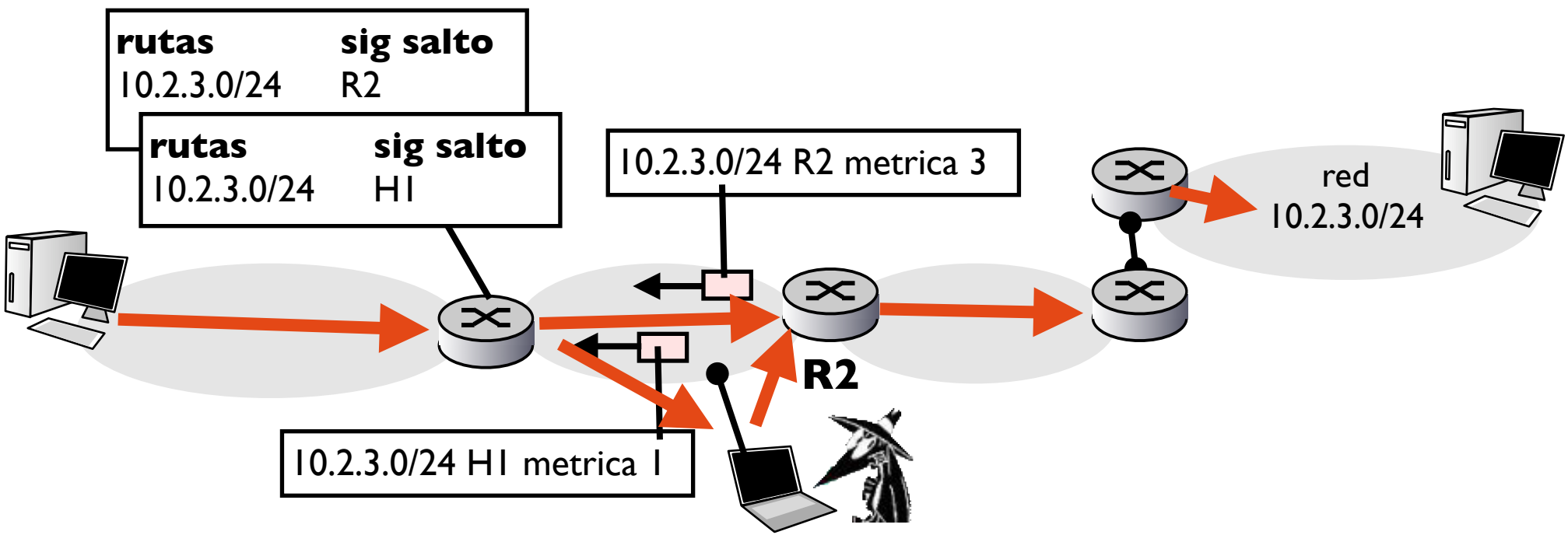
Network hacking: nivel 3

- **IP spoofing**
  - Es fácil enviar paquetes IP con otra dirección IP
  - Util para ocultar ataques de denegación de servicio
  - No es tan fácil usarlo para hacerse pasar por un host. Porque los paquetes de vuelta no vendrán hacia nuestra IP
- **Fragmentación IP**
  - Utilizado para engañar a los firewalls
  - Si un firewall no reconstruye IP no puede analizar TCP/UDP y filtrar por puertos
- **Enrutamiento dinámico**
  - Las tablas de rutas se construyen mediante protocolos de enrutamiento. Los routers vecinos se comunican entre si y se informan de las subredes a las que saben ir.
  - Protocolos de enrutamiento tipicos:

    RIP, OSPF, BGP...
  - Estos protocolos, especialmente los viejos, no están muy pensados para ser seguros

Network hacking: nivel 3

- RIP es un protocolo simple que se usa en redes pequeñas.
  - Basado en UDP (puerto 520)
  - RIPv1 Aceptará cualquier paquete informándole de una ruta suponiendo que el que lo manda es un router
  - Esto se puede usar para lograr redirigir el tráfico



Network hacking: transporte y aplicación

- El nivel de transporte TCP/UDP no cifra los datos
- Muchas aplicaciones de Internet (todas las clásicas) envían los datos sin cifrar confiando en que nadie los leera
- **Sniffer**: programa que examina los paquetes que circulan por la red independientemente de a quien vayan dirigidos (modo promiscuo)
  - Tipicos: Tcpdump, Ethereal
- Se puede obtener mucha información con un sniffer (vease dsniff)
  - Contraseñas de Telnet, FTP, HTTP, correo...
  - Correos electrónicos
  - URIs visitados y contenidos de las páginas
  - Ficheros transferidos o exportados por SMB/NFS
  - Streams de audio/video
- Sniffers orientados a búsqueda de informacion: dsniff
- Sniffers orientados a man-in-the-middle: ettercap (a continuación)
- Sniffers orientados a detección de intrusos: snort (en futuras clases)

Network hacking: TCP

- Técnicas para inyectar datos en una conexión TCP que se está abriendo o para secuestrar una conexión abierta
  - Necesitan predicción de secuencia de TCP
  - Falsificación de IPs (IP spoofing)
  - Usadas para secuestrar una conexión de telnet ya autentificada
  - Ya se usan poco
- Más fácil si puedo hacer pasar el tráfico a través de mi máquina
  - Ettercap: permite man-in-the-middle en conexiones TCP abiertas

Contramedidas

- Sistemas de detección de intrusiones que observen el tráfico en la red local.
- Conmutadores con seguridad de puerto que aseguren que un puerto tiene una MAC concreta
- Conmutadores que permiten hacer redes locales virtuales (VLANs) para separar la red en diferentes LANs
- Uso de aplicaciones que no confíen en que la red no se puede observar. Cifrado a nivel de aplicación
- Uso de técnicas de cifrado a nivel de red: IPsec
- Detección de sniffers
  - se pueden detectar sniffers?

Ataques de denegación de servicio

- Y si el atacante no quiere conseguir acceso?
- Y si sólo quiere interrumpir nuestro servicio?
  - Como venganza
  - Porque es un competidor
  - Porque somos muy visibles y quiere visibilidad
  - ...
- Siempre es mas fácil estropear un sistema que conseguir acceso manteniendo el sistema en funcionamiento

Denial of Service: clasicos

- **Buffer overflow por tamaño de paquete (Ping of death)**
  - Esto colgaba un windows: `ping -l 65510 192.168.1.10`
- **Enviar fragmentos IP solapados**
  - Capaz de gastar todos los recursos de un SO y colgarlo
- **Inundación de Loopback**
  - Si consigo convencer al servicio UDP CHARGEN de que el servicio UDP ECHO de ese mismo ordenador le ha enviado un paquete

    Falsificando un paquete con origen 127.0.0.1 puerto 7 y destino la ip del objetivo y puerto 19

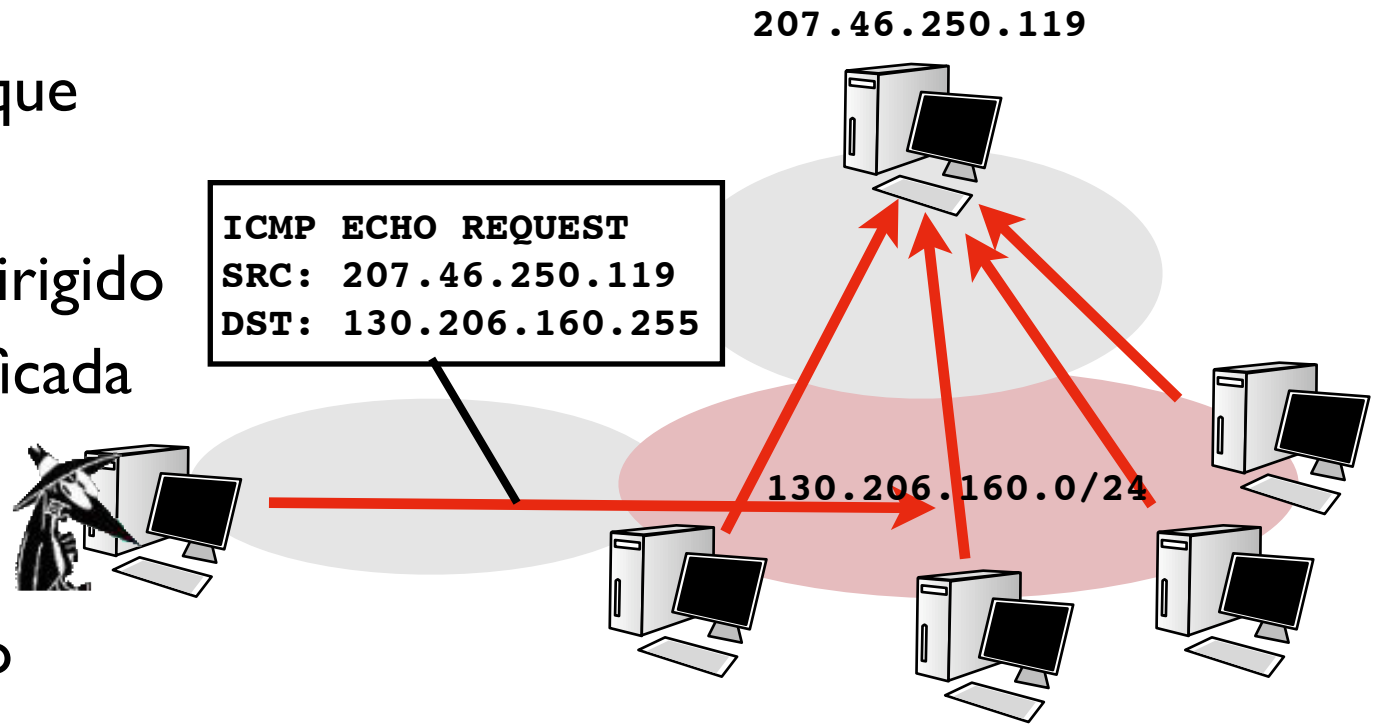
    El destino gastara todos sus recursos en enviarse paquetes a si mismo
- **Nukers**
  - Aprovechando vulnerabilidades de windows que se colgaba si le llegaban paquetes TCP con datos Urgentes
- **Extreme fragmentation** fragmentos idénticos que consumen recursos
- **Vulnerabilidades de NetBIOS** que provocan cuelgues
- **Combos** programas que lanzan todos estos combinados
- **Deben ser tratados como vulnerabilidades a corregir**

Denial of Service: modernos

- Gastar recursos sin explotar vulnerabilidades
- **Inundación de SYNs (SYN flood)**
  - Enviando multiples SYN al mismo puerto desde direcciones IP falsificadas (spoofed)
  - Denegación de servicio sin enviar mucho tráfico. Un usuario con un modem puede parar un servidor Web
- **Inundación con UDP (UDP flood)**
  - Sobrecarga simple de un servicio con paquetes UDP de origen falsificado
  - Es fácil de detectar y solo inunda servicios UDP
  - Además necesitamos más recursos (ancho de banda) que el objetivo atacado...
- **Inundacion con ICMP** (ping -f)

Denial of Service: modernos

- Amplificación del ataque
- **Smurf**
  - Ping a broadcast dirigido
  - Desde una IP falsificada



  - Tráfico amplificado
  - y mas difícil de rastrear
- **Fraggle**
  - Lo mismo pero con paquetes UDP ECHO
- Fueron decayendo conforme los proveedores de servicio comprendían la utilidad de limitar el broadcast dirigido
- Así que los hackers se pasaron al DoS distribuido (DDoS)

Denial of Service Distribuido

- Si no podemos engañar a los ordenadores de una red para que envíen a un destino común mediante un ping broadcast, necesitamos muchos ordenadores para hacer el ataque

  Mejor si no son nuestros

  - Hackers que consiguen acceso a un host e instalan un rootkit

    Tambien instalan un **robot IRC (IRC bot o IRC zombie)**

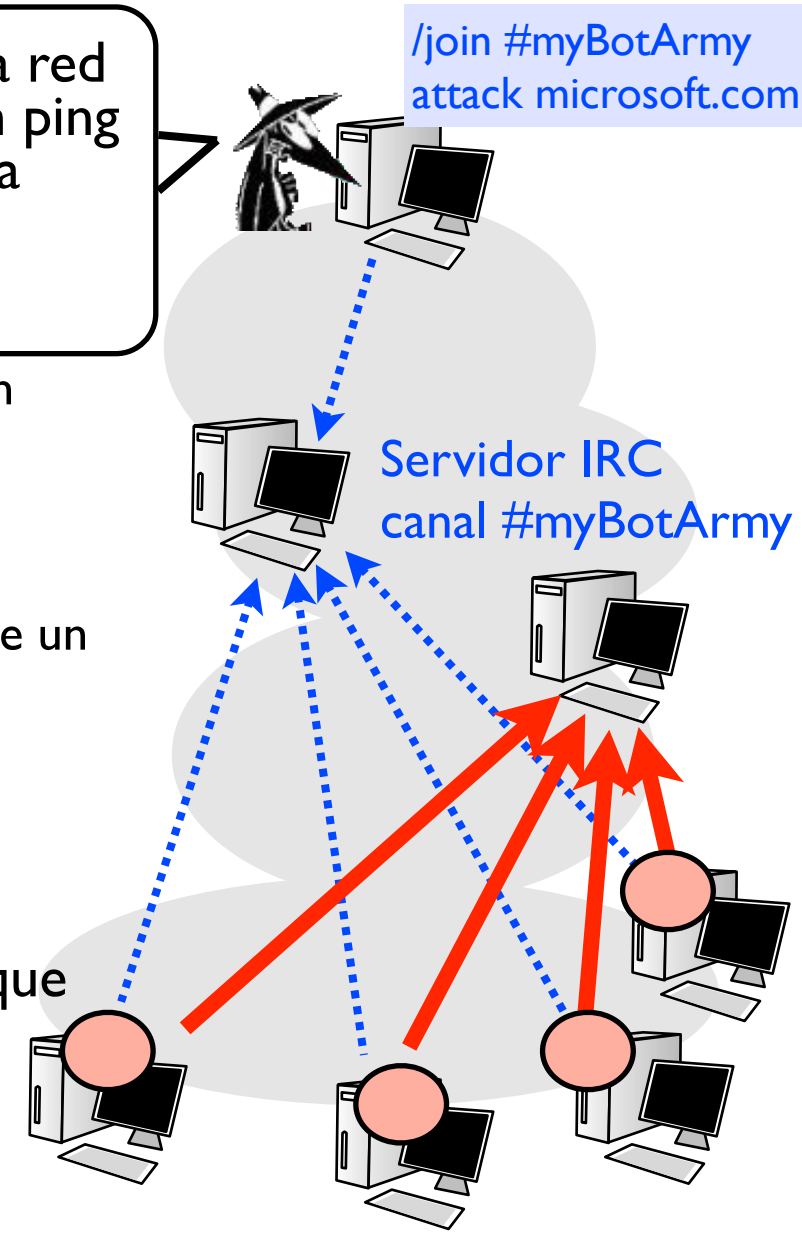
  - También se puede hacer expandiendo el bot mediante un virus o un ataque de ingeniería social por correo

    (mira que guai este programa... tengo que enviarselo a...)

  - El robot se conecta a un canal de IRC predeterminado y espera ordenes

- Las variaciones son infinitas, pero parece que lo que ahora se lleva es el IRC
- Ejercitos de zombies que se compran y venden

  Para esto y también para enviar SPAM



Contramedidas

- Clásicos:
  - Arreglar las vulnerabilidades
- Modernos:
  - Detectar ataques y bloquear las IPs de los que vienen
  - En el fondo es una batalla perdida. La única solución es dimensionar el sistema para que funcione bien a alta carga. Los ataques evolucionan hacia ser usos normales del sistema
  - Detectar el ataque y reaccionar
    - Ser capaz de rastrear el origen
    - Ser capaz de mover el servicio

Conclusiones

- Un hacker conectado a nuestra red puede obtener gran cantidad de información
- Las aplicaciones y servicios de Internet no están muy pensados para ser seguros
- Un administrador de red debe
  - Proteger el acceso a la red para garantizar que no se pueden aplicar estas técnicas desde fuera de la red
  - Vigilar para detectar las intrusiones y ataques que se produzcan desde dentro de su red

- Próxima clase: Sistemas de defensa
- Pendiente: estudio de sistemas de acceso a redes con autentificación