Seguridad en Sistemas Informáticos

Intrusión I: reconocimiento

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

Ataques (intrusion)

- Fases de un ataque
  - Localizando el objetivo y reconocimiento
    - como encontrar un objetivo (footprinting)
    - como explorar la red (scanning)
    - busqueda de vulnerabilidades (enumeration) [*hoy*]
  - Realización del ataque
    - acceso remoto al objetivo
    - escalando privilegios
  - Acceso conseguido
    - cubriendo las huellas
    - plataforma para nuevos ataques [*próxima semana*]
- Otros tipos de ataques (DoS) [*+1 semana*]

Ataques (intrusion)

- **Reconociendo el objetivo**

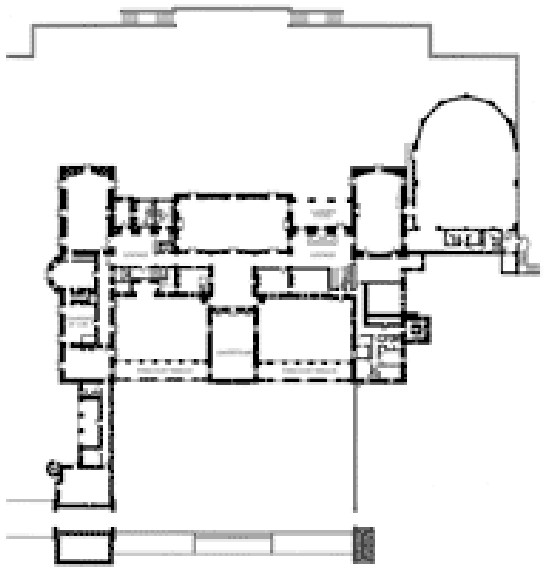
  Obtener toda la información posible

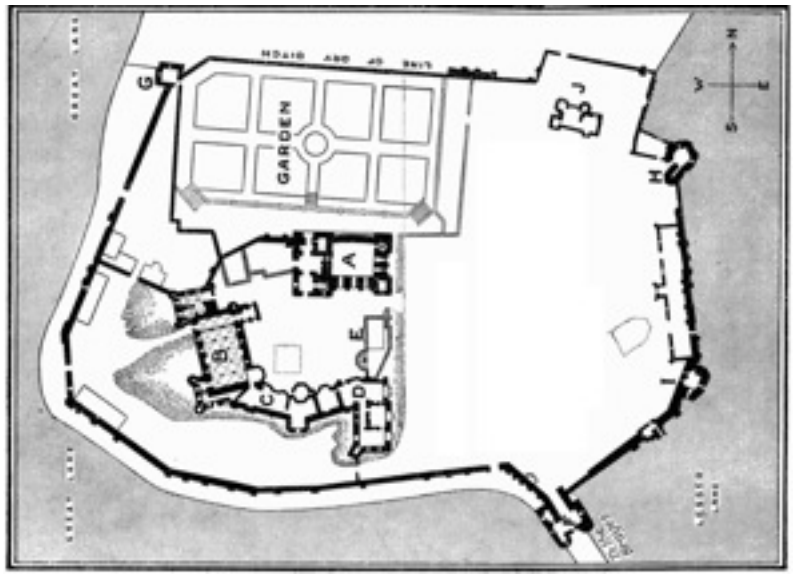
  - Footprinting
    - ¿Qué rango de IPs usa?
    - ¿Cual es su servidor de DNS?
  - Scanning
    - ¿Qué IPs están activas?
  - Enumeration
    - ¿Qué servicios/puertos están activos? (y pueden tener vulnerabilidades)
    - ¿Qué usuarios tienen? (para poder adivinar contraseñas)

Footprinting

- **Footprint**: huella, pero también huella de un edificio o un sistema de comunicaciones

  Huella del objetivo, que extensión ocupa





- ¿Donde están físicamente las redes de mi objetivo?

  ¿Qué rango de IPs ocupa el objetivo?

Footprinting: buscando un poco...

- Información disponible públicamente
  - Pagina web de la empresa
  - Empresas asociadas
  - Localización física (y fotos de satélite en la web)
  - Personas de contacto (con teléfonos, mails y otros detalles)
  - Eventos (compras y fusiones)
  - Políticas de seguridad
  - Información antigua (archivos de la web)
  - Ex-empleados descontentos
  - Ofertas de empleo
  - Foros de ayuda
- Seguro que hay más...

Footprinting: rangos de IP y dominios

- *Internet es en general una red descentralizada...*

  Pero hay cosas que deben centralizarse para asegurar un funcionamiento global
- Las direcciones IPs deben ser únicas
  - Luego alguien mantiene una base de datos de los bloques de direcciones IP asignadas
- Los nombres de dominio
  - Se compran y venden y también deben ser únicos.

- ¿Se puede consultar está información?

  ¿A quién pertenece la IP 130.206.1.1 ?

  ¿Qué direcciones IP tiene asignadas mi objetivo?

Footprinting: rangos de IP y dominios

- ICANN (Internet Corporation for Asigned Names and Numbers)

  http://www.icann.org

  Antes http://www.iana.org
  - Coordina la asignación de direcciones IP
  - Coordina la asignación de nombres
  - Coordina la asignación de puertos y otros números para protocolos
- **Servicio de consulta WHOIS (who is?)**
  - Servicio WHOIS (sobre TCP puerto 43)
    - `whois 130.206.1.1`
    - `whois www.skype.com`
  - Ahora también en página web
  - Pero no es tan centralizado...

Organización de las IPs

- ICANN asigna bloques de direcciones a los Registros de Internet Regionales
  - APNIC: región Asia/Pacifico (http://www.apnic.net)
  - ARIN: America y Afria Subsahariana (http://www.arin.net)
  - LACNIC: Latinoamerica y Caribe (http://www.lacnic.net)
  - RIPE: Europa, partes de Asia, norte de Africa y Oriente Medio (http://www.ripe.net)
  - AfriNIC: Africa, eventualmente asumira el control de las regiones de Africa controladas por ARIN y RIPE (http://www.afrinic.net)
- Lo que nos interesa es que cuando queremos localizar una IP o un dominio tendremos que preguntar en varios servidores

Buscando un dominio

- En http://www.nic.es buscamos unavarra.es

DATOS DEL TITULAR	
Nombre del dominio	unavarra.es
Titular	Universidad Publica de Navarra
Tipo de Titular	Organización
Forma Jurídica	Otras
Domicilio	Campus Arrosadia
Población	Pamplona
Provincia	NAVARRA
Código Postal	E-31006
País	España
Marca	
Número de Inscripción de la Marca	
Fecha de Alta	26/03/1998
Fecha Caducidad	26/03/2007
Agente Registrador	Nominalia

Dirección física

Buscando un dominio

- Información de administradores

  Nombres y teléfonos
- Posibilidad de Ingeniería social

PERSONA DE CONTACTO ADMINISTRATIVO

NIC_HANDLE	**FJAP1-ESNIC**
Nombre	**Francisco Jose Abadia Perez**
Organización	Universidad Publica de Navarra
Email	arm@unavarra.es
Teléfono	34 948169090
Domicilio	Campus Arrosadia
Población	Pamplona
Provincia	NAVARRA
Código Postal	31006
País	España

PERSONA DE CONTACTO TECNICO

NIC_HANDLE	**JFL3-ESNIC**
Nombre	**Javier Fernandez Landa**
Organización	Universidad Publica de Navarra
Email	javier.fernandez@unavarra.es
Teléfono	34 948169088
Domicilio	Campus Arrosadia
Población	Pamplona
Provincia	NAVARRA
Código Postal	E-31006
País	España

Ir

Buscando un dominio

- Direccion de servidores de DNS

SERVIDORES DNS	
Nombre Servidor	**IP**
dns2.unavarra.es	130.206.166.109
chico.rediris.es	130.206.1.3
sun.rediris.es	130.206.1.2
dns1.unavarra.es	130.206.158.254

- Rangos de direcciones

```
$ whois 130.206.166.109
...
% Information related to '130.206.0.0/16AS766'
route:          130.206.0.0/16
descr:          IRIS
origin:         AS766
mnt-by:         REDIRIS-NMC
source:         RIPE # Filtered
```

Footprinting: rangos de IP y dominios

- Base de datos distribuida del DNS
  - Servidores raiz (quien es el servidor de DNS de cada dominio)
  - Servidores de un dominio (nombres e IPs de una organizacion)
- Consultando el DNS
  - nslookup nombre [servidor]
  - nslookup direccionip [servidor]

```
$ nslookup - dns1.unavarra.es
> mikel.tlm.unavarra.es
Server:         dns1.unavarra.es
Address:        130.206.166.110#53

Name:   mikel.tlm.unavarra.es
Address: 130.206.169.177
>
```

- Averiguar todos los nombres es cuestión de paciencia o scripting

DNS y zone transfers

- En DNS se puede configurar servidores redundantes
  - Los servidores de DNS se actualizan mediante una operación de petición de DNS denominada Zone Transfer
  - Un servidor de DNS incorrectamente configurado puede enviar la Zone Transfer a cualquiera que lo pida

    Que consigue la lista de todos las direcciones IP y nombres del dominio

```
$ dig -t axfr dns1.unavarra.es

; <<>> DiG 9.2.2 <<>> -t axfr dns1.unavarra.es
;; global options:  printcmd
; Transfer failed.
```

Reconocimiento de red

- ping y traceroute
  - Herramientas utiles para el administrador de la red
- Pero también pueden usarse para obtener información desde fuera
  - traceroute -n -p 53 159.237.12.60

```
$ traceroute -n -p 53 159.237.12.60
traceroute to 159.237.12.60 (159.237.12.60), 64 hops max, 40 byte packets
 1  192.168.2.2  2.637 ms  27.932 ms  1.560 ms
 2  192.168.1.1  2.856 ms  2.228 ms  2.806 ms
 3  192.168.153.1  259.148 ms  270.419 ms  490.018 ms
 4  80.58.114.97  489.759 ms  513.038 ms  45.081 ms
 5  80.58.73.118  62.692 ms  63.063 ms  63.908 ms
 6  193.149.1.154  67.559 ms  63.137 ms  63.461 ms
 7  130.206.240.125  65.608 ms  63.852 ms  64.065 ms
 8  130.206.240.2  63.901 ms  63.869 ms  64.463 ms
 9  130.206.240.30  78.135 ms  78.596 ms  115.834 ms
10  130.206.240.62  83.030 ms  83.135 ms  84.441 ms
11  130.206.209.2  84.968 ms  83.617 ms  83.332 ms
12  159.237.4.2  90.526 ms  79.444 ms  79.200 ms
13  159.237.12.60  83.097 ms  84.040 ms  84.128 ms
```

Y esto parece el router de entrada

Está funcionando

Contramedidas

- Alguna información tiene que ser publica y no se puede hacer nada
  - Cuidar lo que se revela en foros y usar alias
  - Prepararse para ataques de ingenieria social al teléfono
- Mantener actualizada la información de dominio y cuidado con el secuestro de dominios
- DNS restringir zone transfers
- Bloquear ICMP en el borde de la red? (controvertido)

Scanning

- **Scan**: the act of examining sequentially, part by part
- En RADAR enviar energía hacia una parte especifica para ver que vuelve... y poder decir que hay algo ahi

- Examinar el área del objetivo y encontrar todas su partes: máquinas, direcciones IP...
- Pasamos al examen **activo** (=detectable)

Como conseguir una lista de IPs?

- Red C del DNS, o de un servidor conocido
  - Pero no sabemos si hay un ordenador en la IP aunque este reservada
- traceroutes
  - Sólo vemos las IPs del camino
- **Técnica básica: Barrido de pings**
- ping broadcast

  Suele estar cortado y no se puede hacer desde fuera de la red
- sniffer

  Solo vale si estas dentro de la red para detectar a los que hacen tráfico

Barrido de pings

- Dada una lista de IPs comprobar en cual de ellas hay un IP escuchando es fácil: enviar ICMP pings
- Scripts hgalo usted mismo
  - ping es un poco dificil de scriptar
  - fping está más pensado para eso

```
$ fping <fichero_con_ips
130.206.160.1 is alive
130.206.160.2 is alive
130.206.160.10 is alive

$ ( i=1; while [[ $i -le 254 ]] ; do echo 130.206.160.$i ;
i=$(( $i + 1 )); done ) | sudo fping -a
130.206.160.1 is alive
130.206.160.2 is alive
130.206.160.10 is alive
...
```

Barrido de pings

- Herramienta por excelencia para escanear: **nmap**

  barrido de pings con

-sP = ping scan

red especificada como CIDR

```
$ nmap -sP 130.206.160.0/28
Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2006-10-02 18:40 CEST
Host arce-un.red.unavarra.es (130.206.160.1) appears to be up.
Host brezo-un.red.unavarra.es (130.206.160.2) appears to be up.
Host s160m12.unavarra.es (130.206.160.12) appears to be up.
Nmap finished: 16 IP addresses (3 hosts up) scanned in 0.266 seconds
```

-n para que no busque la informacion de DNS
no queremos saber el nombre
y eso genera más trafico = menos discreto

- Hay también muchas herramientas con interfaz gráfico: SuperScan for windows

Respuestas a ICMP

- Provocar otras respuestas ICMP diferentes del ICMP ECHO REPLY también puede proporcionar informacion
  - Eso es lo que hace traceroute con el ICMP TTL EXCEDED
- Más usos (vease icmpquery)
  - ICMP TIMESTAMP para conseguir la hora del router
  - ICMP ADDRESS MASK para conseguir la mascara de un interfaz

Contramedidas

- Decidir que mensajes ICMP se filtran en el borde de la red
- Monitorizar la red y observar los ICMPs

scaners mas discretos

- Los monitorizadores de red pueden buscar patrones que indiquen el barrido y hacer sonar alarmas
- Técnicas para ser más discretos
  - No hacer los pings secuencialmente sino aleatoriamente
  - No hacer los pings demasiado rápido
  - Falsificar la dirección de origen
    - Hacer pings desde varias direcciones muchas falsas y una verdadera (hace falta una verdadera para enterarme de quien responde)
  - No usar ICMP
    - ¿Que otra cosa podemos usar?

Contramedidas

- **Detección**
  - Los barridos se pueden detectar y pueden indicar ataques posteriores
  - Programas para detectarlos en un host (Genius)
  - Detección y alarmas en Firewalls e IDS
  - Detectando barridos camuflados (investigación)
- **Prevención**
  - Reconsiderar que trafico ICMP intercambiamos con el exterior. (ECHO, PORT_UNREACHABLE y TTL_EXCEDED)
  - Según necesidades de seguridad restringirlo todo o restringir IPs que pueden hacer
  - Reacción automática ante barridos (investigación)

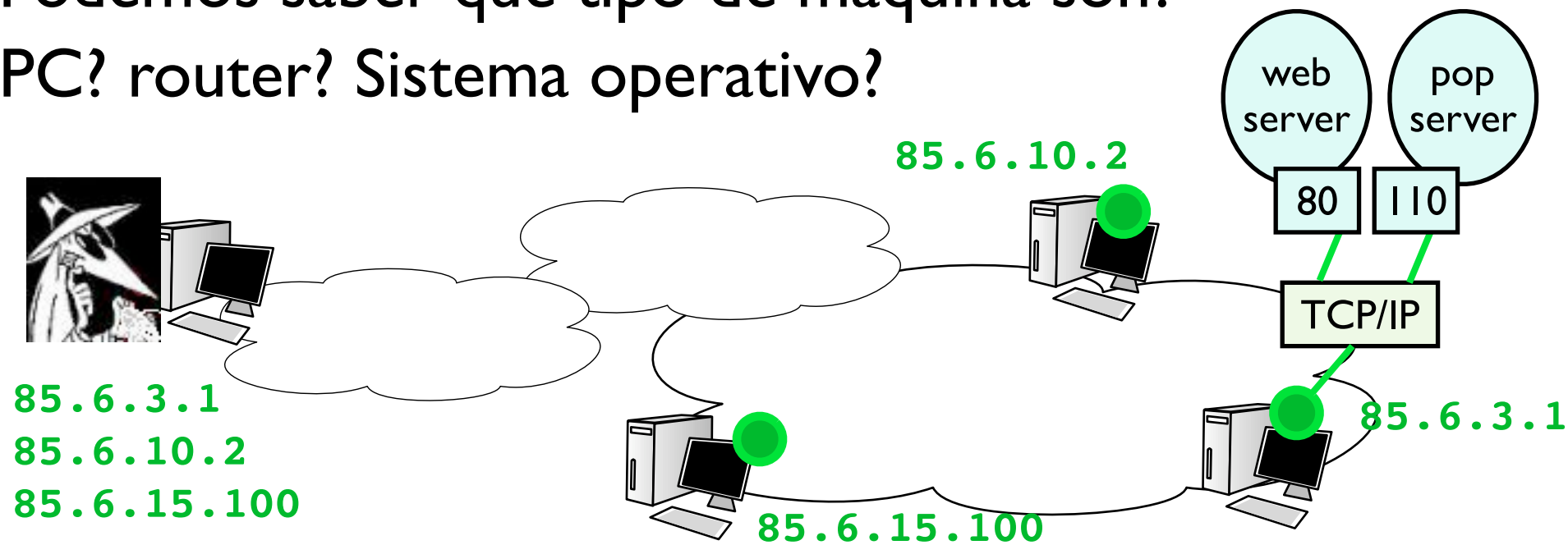
Enumeración

- A partir de una lista de IPs, para las IPs objetivo
- Enumerar posibles puntos de entrada a cada máquina
  - Puertos y servicios que usan
  - Vulnerabilidades: que versión del sistema operativo y del programa servidor usa?
  - Cualquier cosa extra que pueda ayudar

    nombres de usuarios, nombres de directorios...

Puertos abiertos

- Una vez que sabemos donde están las máquinas
- Qué programas corren en las máquinas
  - En que puertos hay servidores escuchando?
    usando **`telnet` o `nc`**
- Podemos saber que tipo de máquina son?
  PC? router? Sistema operativo?



Recuerde uso de telnet y nc

- Probando un puerto abierto
- Con telnet

```
$ telnet www.google.com 80
Trying 66.102.9.99...
Connected to www.l.google.com.
Escape character is '^]'.
```

Puerto escuchando

```
$ telnet 192.168.1.1 25
Trying 192.168.1.1...
telnet: connect to address 192.168.1.1: Connection refused
telnet: Unable to connect to remote host
```

Puerto no escuchando

```
$ telnet www.google.com 25
Trying 66.102.9.99...
telnet: connect to address 66.102.9.99: Operation timed out
```

Y si hay timeout???

Recuerde uso de telnet y nc

- Probando un puerto abierto
- Con nc

-v para que diga si se ha conectado
-n para que no consulte el DNS

```
$ nc -v -n 66.102.9.147 80
(UNKNOWN) [66.102.9.147] 80 (?) open

$ nc -v -n 192.168.1.1 25
(UNKNOWN) [192.168.1.1] 25 (?) : Connection refused
```

- Pero nc tiene también modo port scanner !!

```
$ nc -z -w2 -v -n 192.168.1.1 1-1000
(UNKNOWN) [192.168.1.1] 80 (?) open
(UNKNOWN) [192.168.1.1] 23 (?) open
(UNKNOWN) [192.168.1.1] 21 (?) open
```

-z no esperes input del usuario
-w<t> tiempo a esperar intentando

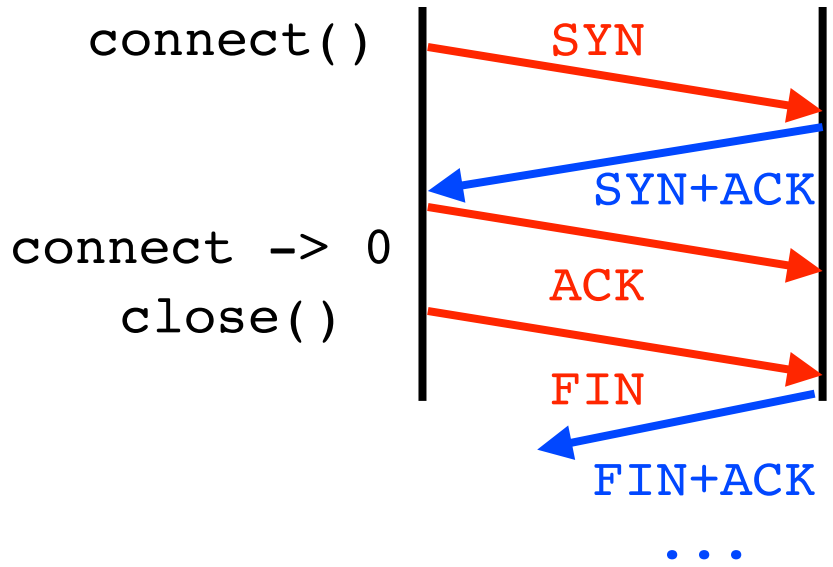
Buscando servicios

- Determinar si un puerto está abierto en una máquina remota
  - Intentar una conexión

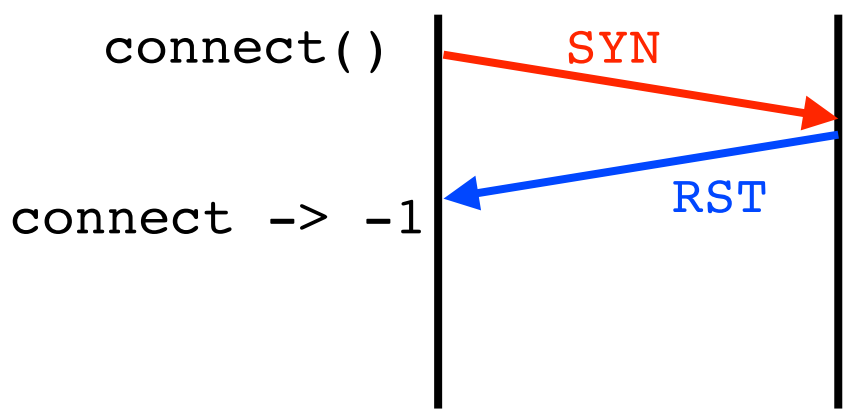
    si se completa la cerramos y había servidor
- Es fácil hacer un programa que haga esto a un rango de puertos

  (como nc)

Hay servidor



No hay servidor

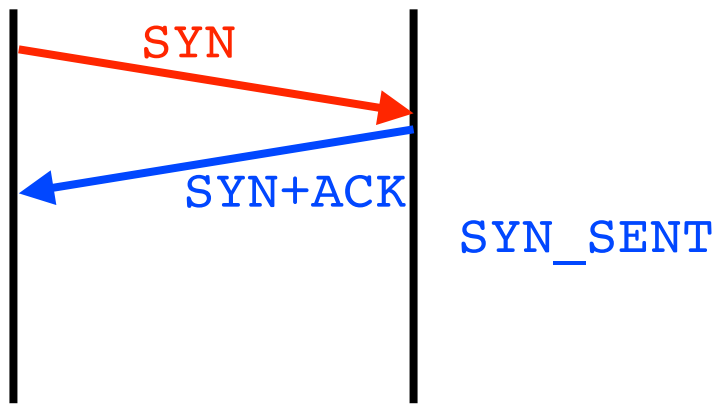


Buscando servicios (con discreción)

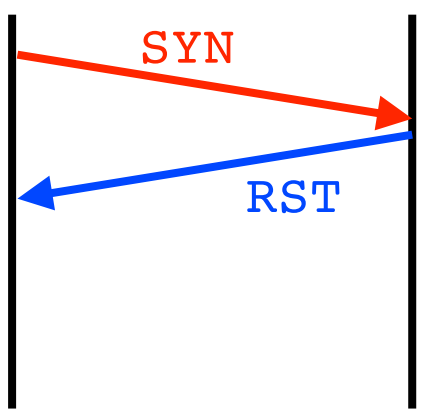
- Mas maleducado

  y discreto
  - Enviar un SYN pero no completar el establecimiento
  - El servidor queda en SYN_SENT
  - Denegacion de Servicio (si se lo haces a muchos puertos a la vez)
- 3 posibles resultados
  - vuelve SYN+ACK
  - vuelve RST
  - no vuelve nada (firewall)

Hay servidor



No hay servidor



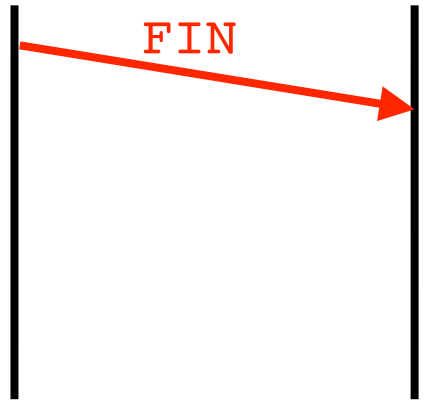
Buscando servicios (con discreción)

- Enviando paquetes raros
  - Un FIN aunque no haya conexion
  - Un paquete XmasTree (todos los flags)
  - Un paquete null (ningun flag)
  - Si no hay servidor en ese puerto se envia RST.
    Si hay servidores ignorar

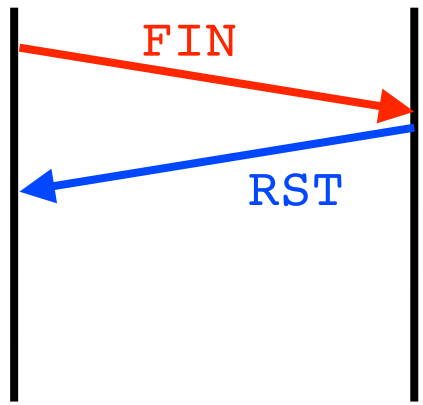
    (vease RFC-793 TCP)
  - Indicador de puerto abierto
- Mas discreto
- Menos información

  no puede distinguir el puerto con un servidor de que haya un firewall (en ningún caso vuelve paquete)

Hay servidor



No hay servidor



Buscando servicios (en UDP)

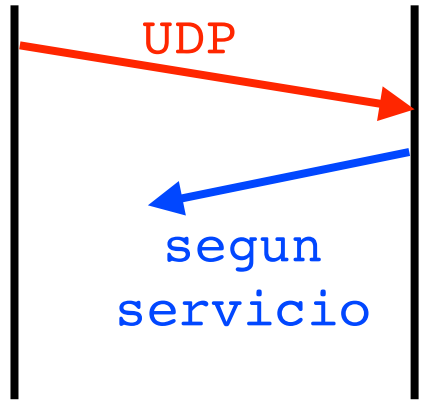
- Enviando paquetes UDP al servidor
  - si hay servidor contestara
  - o no enviara nada segun el protocolo
  - Si no hay servidor en ese puerto

    se envía un error ICMP

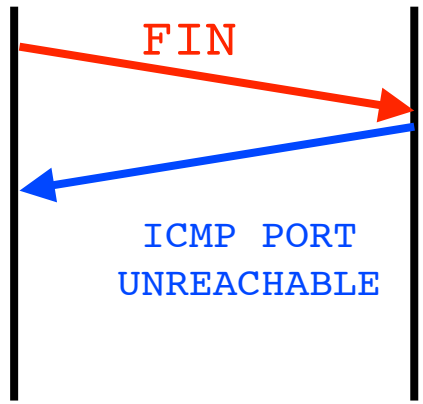
- Problema distinguir OPEN y FILTERED

- Se puede usar para escanear máquinas más discretamente que con ICMP
- Se puede mandar UDP a broadcast o multicast

Hay servidor



No hay servidor



Network Maper (nmap)

- Realiza

  -sP escaneo de IPs con pings

  -sT escaneo de puertos TCP conexión completa

  -sS escaneo de TCP con SYN solo

  -sF -sX -sN escaneo con Fin XmasTree o Null

  -sU escaneo en UDP

  -p rango de puertos (si no escanea todos)

  direccion IP una o una subred

  -P0 no hace ping y pasa directamente al scan

  -v verbose -n no hagas DNS

  -Dip1,ip2,ip3 genera escaneos falsos de otras direcciones

  > Y una cosa mas...

Fingerprinting

- Se puede averiguar que sistema operativo usa una IP? (fingerprinting)
- Sería muy util
  - Para obtener el máximo de información sobre una máquina
  - Porque las vulnerabilidades dependerán del sistema operativo
- Hay varias maneras
  - A veces no hay que esforzarse mucho. Basta con ver que puertos tiene abiertos o con hacerle telnet o FTP

```
$ telnet 10.1.1.12
Trying 10.1.1.12...
Connected to 10.1.1.12.
Escape character is '^]'.

Red Hat Linux release 6.1 (Cartman)
Kernel 2.2.12-20 on an i686
login:
```

Algunas cosas no han cambiado desde los primeros tiempos de Internet

  - Pero se puede sacar esta información solo de TCP/IP ???

Fingerprinting activo

- Las implementaciones de TCP/IP no son todas iguales

  Los estándares y RFCs no especifican todos los detalles y dejan algunas cosas a la implementacion
- Observando el comportamiento ante ciertas situaciones poco comunes (enviar ciertos paquetes y observar como reacciona la pila TCP/IP del destino) podemos hacernos una idea de que implementación y que sistema operativo es
- Opción -O de nmap

```
$ sudo nmap -p80-100 -O 130.206.169.213

Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2006-10-03 14:47 CEST
Interesting ports on silicon9.unavarra.es (130.206.169.213):
(The 20 ports scanned but not shown below are in state: closed)
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:14:51:22:72:76 (Unknown)
Device type: general purpose
Running: Apple Mac OS X 10.3.X
OS details: Apple Mac OS X 10.3.0 - 10.3.3

Nmap finished: 1 IP address (1 host up) scanned in 2.995 seconds
```

Fingerprinting pasivo

- El fingerprinting activo puede ser detectado
- Hay variaciones de la implementación que pueden ser detectadas pasivamente
  - TTL utilizado en los paquetes que envía
  - Tamaño de ventana que envía al iniciar conexión
  - Envía el flag No Fragmentar?
- Programa siphon, un poco viejo
- Heredero: p0f

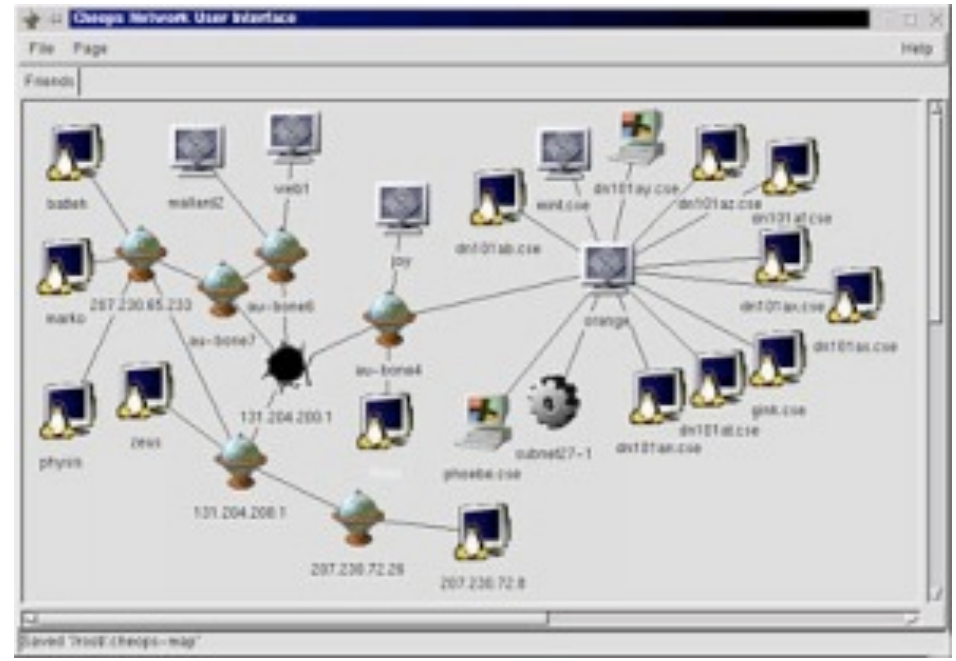
```
# Window:TTL:DF:Operating System
# DF = 1 for ON, 0 for OFF.

7D78:64:1:Linux 2.1.122 - 2.2.14
77C4:64:1:Linux 2.1.122 - 2.2.14
7BF0:64:1:Linux 2.1.122 - 2.2.14
7BC0:64:1:Linux 2.1.122 - 2.2.14
```

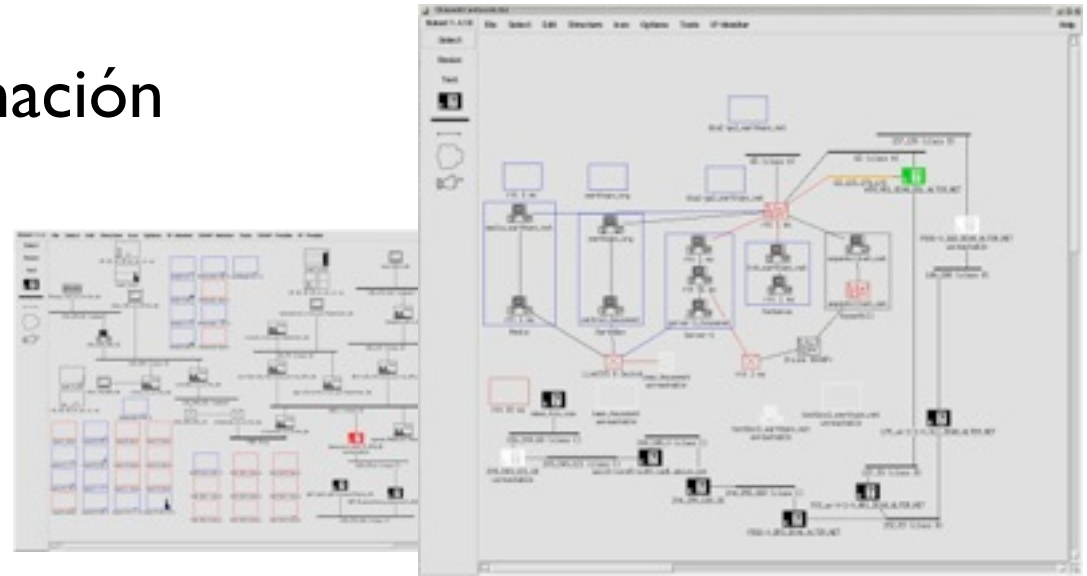
```
$ sudo p0f -NU -i en0
p0f - passive os fingerprinting utility, version 2.0.8
(C) M. Zalewski <lcamtuf@dione.cc>, W. Stearns <wstearns@pobox.com>
p0f: listening (SYN) on 'en0', 262 sigs (14 generic, cksum 0F1F5CA2), rule: 'all'.
85.19.153.10:2950 - Windows 2000 SP4, XP SP1+
130.206.169.213:54336 - FreeBSD 6.x (2) (up: 902 hrs)
220.225.242.235:62504 - Windows 2000 SP4, XP SP1+
```

Todo en uno

- Cheops (cheops-ng)
  - Dibuja la red que ve basado principalmente en nmap con interfaz gráfico



- Tkined
  - Recopila información por SNMP



Más enumeración

- Banner grabbing

  guardar lo que llega por las conexiones de los servicios clasicos: Web, Telnet, FTP, SMTP... dicen el servidor y el sistema
- Servicios Finger, Rwho dan informacion sobre usuarios de Unix
- SNMP gestión de equipos de red da información de configuración
- MSRPC, NetBios, SMB enumeración de directorios compartidos
- NFS enumeración de directorios
- En general todos los basados en RPC o MSRPC
- ActiveDirectory enumeración de usuarios

- Vea la bibliografía para técnicas concretas y herramientas
- Conclusión: no deje abiertos servicios que no necesite

Contramedidas

- Detección
  - Igual que los barridos, se pueden detectar

    Técnicas de detección y camuflaje en evolución
- Prevención
  - Asumir que si hay un puerto abierto se encontrará
  - Llevar control: Que no haya puertos abiertos que conozcan los hackers y no el administrador
  - No tener servicios innecesarios activados

    Minimizar la superficie de ataque
  - Filtrar acceso a servicios peligrosos desde fuera de su red

Y si no tengo un objetivo

- Me da igual cualquier ordenador que tenga la vulnerabilidad X
- Scanner que buscan una vulnerabilidad
  - Escanear IPs con conexiones al puerto del ataque
  - Ejemplo W32.Blaster.Worm y otros gusanos

    http://www.symantec.com/security_response/writeup.jsp?docid=2003-081113-0229-99&tabid=2
  - Ejemplos ataques a servidores web
- Google hacking

  google ya ha escaneado millones de servidores web !!
  - Buscando: Welcome to IIS 4.0
  - Buscando: "VNC Desktop" inurl:5800
  - Buscando: filetype:bak htpasswd

Conclusiones

- Técnicas para obtener una visión de la red del objetivo
  - Mucho que averiguar de forma pasiva
    (nadie tiene por que enterarse...)
  - Mucho que averiguar de forma activa pero inocente
    (no estoy haciendo nada malo...)
- Contramedidas
  - Saber que información es pública
  - No dejar abiertos servicios no esenciales
  - Hacer auto reconocimiento y auditoría
- Siguiente clase: Pasando al ataque...
  Intrusión 2: consiguiendo acceso