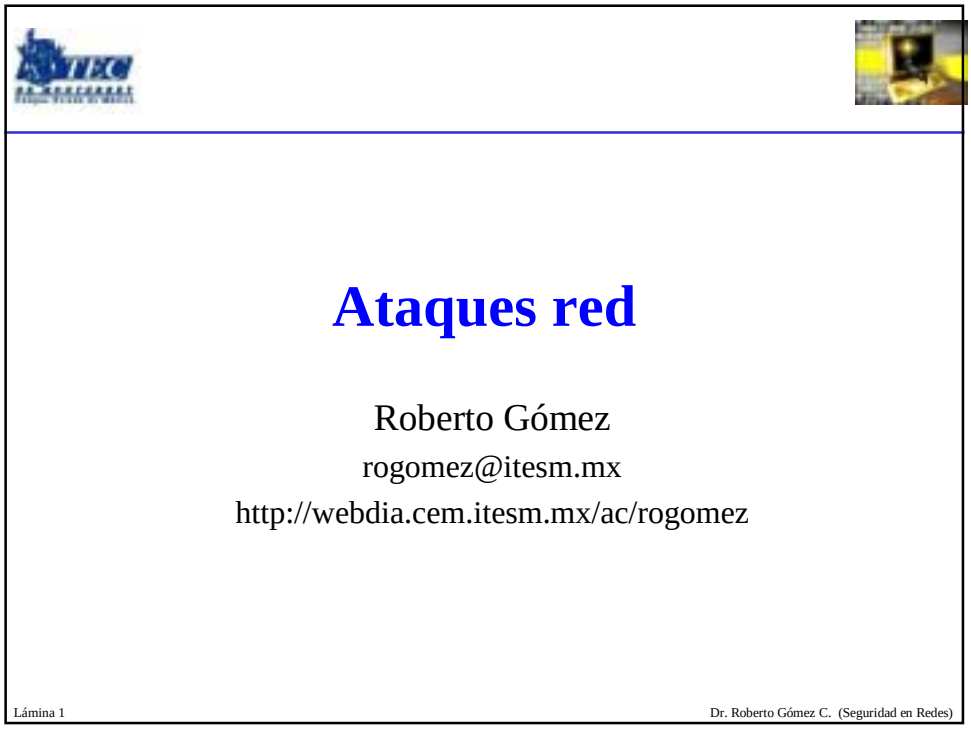
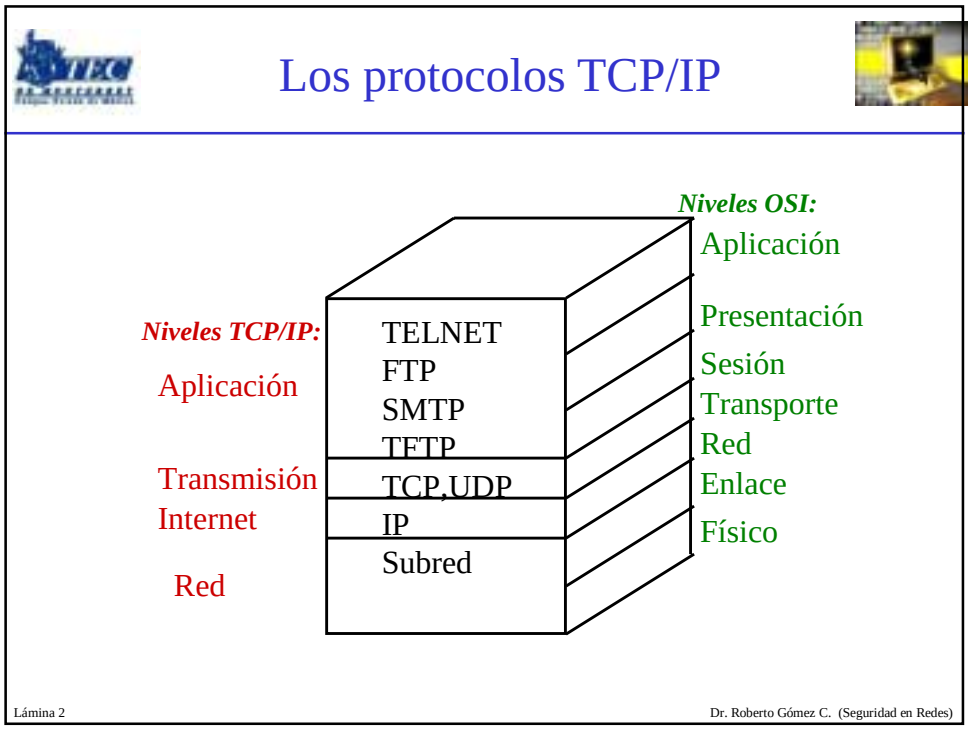
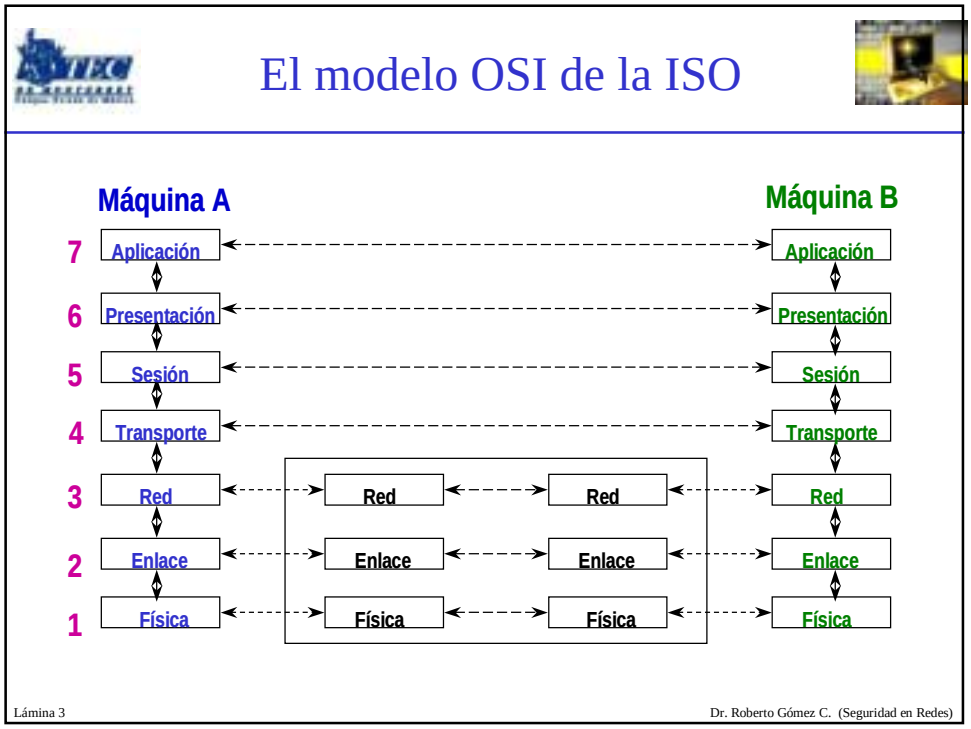
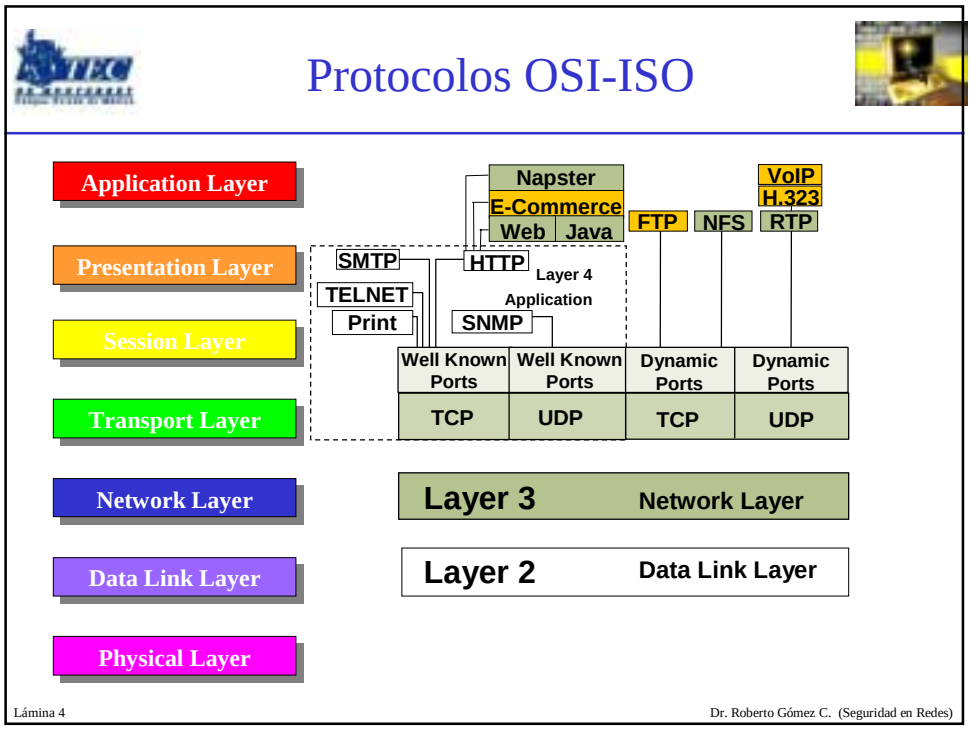

Ataques red
Roberto Gómez
rogomez@itesm.mx
http://webdia.cem.itesm.mx/ac/rogomez
Lámina 1
Dr. Roberto Gómez C. (Seguridad en Redes)


Los protocolos TCP/IP
Niveles OSI:
Aplicación
Presentación
Sesión
Transporte
Red
Enlace
Físico
Niveles TCP/IP:
Aplicación
Transmisión
Internet
Red
TELNET
FTP
SMTP
TFTP
TCP,UDP
IP
Subred
Lámina 2
Dr. Roberto Gómez C. (Seguridad en Redes)


El modelo OSI de la ISO
Máquina A
Máquina B
7 Aplicación
6 Presentación
5 Sesión
4 Transporte
3 Red
2 Enlace
1 Física
Red
Enlace
Física
Lámina 3
Dr. Roberto Gómez C. (Seguridad en Redes)


Protocolos OSI-ISO
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer
Napster
E-Commerce
Web
Java
VoIP
H.323
FTP
NFS
RTP
SMTP
HTTP
TELNET
Print
SNMP
Layer 4
Application
Well Known Ports
Well Known Ports
Dynamic Ports
Dynamic Ports
TCP
UDP
TCP
UDP
Layer 3
Network Layer
Layer 2
Data Link Layer
Lámina 4
Dr. Roberto Gómez C. (Seguridad en Redes)

Direcciones MAC y tablas CAM

48 bits hexadecimales (base 16)

1234.5678.9ABC

Primeros 24 bits = Código Fabricante asignado por la IEEE

0000.0cXX.XXXX

Segundos 24 bits = Interfaz Específica asignado por el fabricante

XXXX.XX00.0001

Todos F's = Broadcast

FFFF.FFFF.FFFF

- Tablas CAM: Content Addressable Memory.
- Tabla almacena información como direcciones MAC disponibles en los puertos físicos con sus parámetros de VLAN asociados.
- Las tablas tienen un tamaño fijo.

Lámina 5 Dr. Roberto Gómez C. (Seguridad en Redes)

Comportamiento normal CAM 1/3

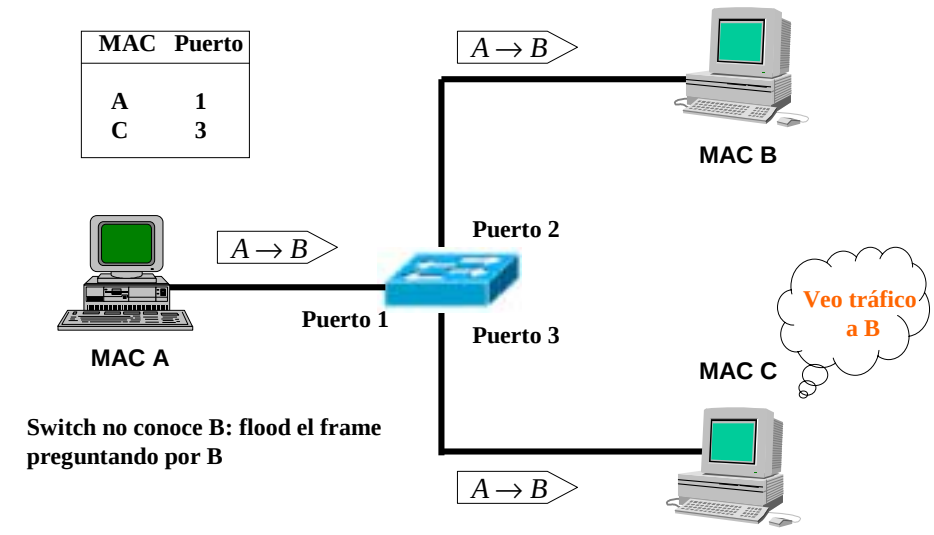
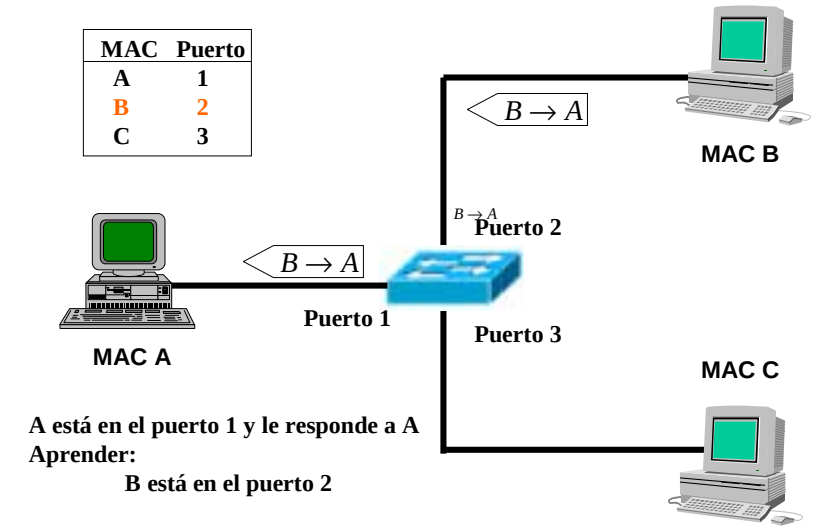


Lámina 6 Dr. Roberto Gómez C. (Seguridad en Redes)

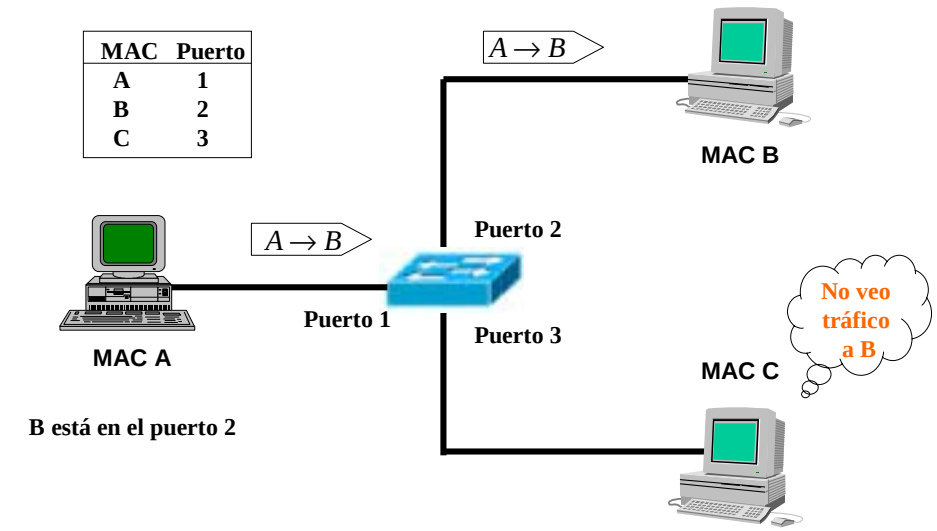
Comportamiento normal CAM 2/3



A está en el puerto 1 y le responde a A
Aprender:
B está en el puerto 2

Lámina 7
Dr. Roberto Gómez C. (Seguridad en Redes)

Comportamiento normal CAM 3/3



B está en el puerto 2

Lámina 8
Dr. Roberto Gómez C. (Seguridad en Redes)

Overflow del CAM

- Ataque teórico hasta mayo 1999
- Herramienta macof desde mayo 1999
  - aproximadamente 100 líneas de Perl
- Se aprovecha del tamaño fijo de la tabla de CAM

Catalyst CAM Tables

- Switches catalyst usan hash para dar de alta MACs en una tabla CAM

1	A	B	C					
2	D	E	F	G				
3	H							
:	I							
:	J	K						
16,000	L	M	N	O	P	Q	R	S

T inundando

- 63 bits de fuente (MAC, VLAN, misc) crea un valor hash de 17 bits
  - si el valor es el mismo (colisión) existen 8 columnas para ubicar entradas CAM, si las 8 están llenas el paquete inunda la VLAN

Llenando la tabla CAM

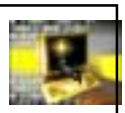
- Dsniff (macof) puede generar 155,000 entradas MAC por minuto en un switch.
- Asumiendo una función hash perfecta la tabla CAM se llenará después de 128,000 direcciones (16,000 x 8 = 31,052 para ser exactos).
- La función hash no es perfecta
  - actualmente toma 70 segundos llenar la tabla CAM

CAT6506 (enable) sho cam count dynamic
Total Matching CAM entries = 131052

- Una vez que la tabla esta llena, tráfico sin una entrada CAM inunda la VLAN, pero no existe tráfico con una entrada en la tabla CAM

Lámina 11
Dr. Roberto Gómez C. (Seguridad en Redes)

Dsniff



- Es una colección de herramientas que pueden implementar diferentes ataques.
- Realizado por Dug Song
- ARP spoofing
- MAC flooding
- Selective sniffing
- SSH/SSL interception

Lámina 12
Dr. Roberto Gómez C. (Seguridad en Redes)

Atacando el problema

- Port Security
  - Sus capacidades dependen de la plataforma
  - Permite especificar direcciones MAC para cada puerto, o aprender un cierto número de direcciones MAC por puerto
  - Una vez detectada una dirección MAC invalida el switch puede configurarse para bloquear solo la MAC causante del problema o dar de baja el puerto
  - Previene que macof inunde la tabla CAM

Lámina 13 Dr. Roberto Gómez C. (Seguridad en Redes)

Negación de servicio

- Su objetivo principal es impedir que un organismo proporcione el servicio para el que fue creado.
  - busca elevar los índices de utilización de algún servicio o sistema hasta bloquear totalmente el acceso al mismo desde el exterior
- Generalmente se basa en un ataque a una sola máquina
- Un ataque de DoS desorganiza o niega completamente un servicio a los usuarios legítimos
- Por regla general es más fácil realizar un ataque de DoS que introducirse en un sistema
- Es más fácil esconder el origen de un ataque de DoS

Lámina 14 Dr. Roberto Gómez C. (Seguridad en Redes)

Algunos tipos negación servicio

- Consumo de Ancho de Banda
- Inanición de recursos
- Defectos de programación
- Paquetes mal formados
- Ataques DNS y de enrutamiento

Lámina 15 Dr. Roberto Gómez C. (Seguridad en Redes)

Consumo ancho banda

- Buscan consumir todo el ancho de banda disponible
- Pueden definirse 2 escenarios
  1. Los atacantes buscan inundar la conexión de la red de la víctima utilizando un ancho de banda disponible mayor.
  2. El atacante une multitud de sitios para inundar la conexión de la víctima. El atacante hará que varios sitios envíen información de forma concentrada hacia la red víctima.

Lámina 16 Dr. Roberto Gómez C. (Seguridad en Redes)

Inanición de recursos

- Está enfocado al consumo de recursos del sistema.
- Los recursos abusados pueden ser:
  - CPU
  - Memoria
  - Cuotas del Sistema de Archivos
  - Número de proceso
  - Capacidad de un servicio
- Muchos virus distribuidos por email realizan su ataque de esta forma

Lámina 17 Dr. Roberto Gómez C. (Seguridad en Redes)

Defectos de programación

- Son fallos de una aplicación, sistema operativo o elemento de hardware
- Estos fallos tienden a ocurrir cuando un usuario envía datos imprevistos al elemento vulnerable.
- Ejemplo:
  - Paquetes ICMP mal formados
  - Mensajes TCP de longitud anormal
  - Ejecución de instrucciones erróneas

Lámina 18 Dr. Roberto Gómez C. (Seguridad en Redes)

Paquetes Mal Formados

- Una de las formas más comunes de detener un servicio.
- Explotan un error en el stack TCP/IP de la máquina destino enviando uno o más paquetes, mal formados, a la máquina destino.
- Si la maquina destino es vulnerable es posible que:
  - termine con un proceso
  - toda la red de comunicaciones
  - provocar que el sistema operativo de la victima se detenga

Lámina 19
Dr. Roberto Gómez C. (Seguridad en Redes)

Banderas Encabezado TCP

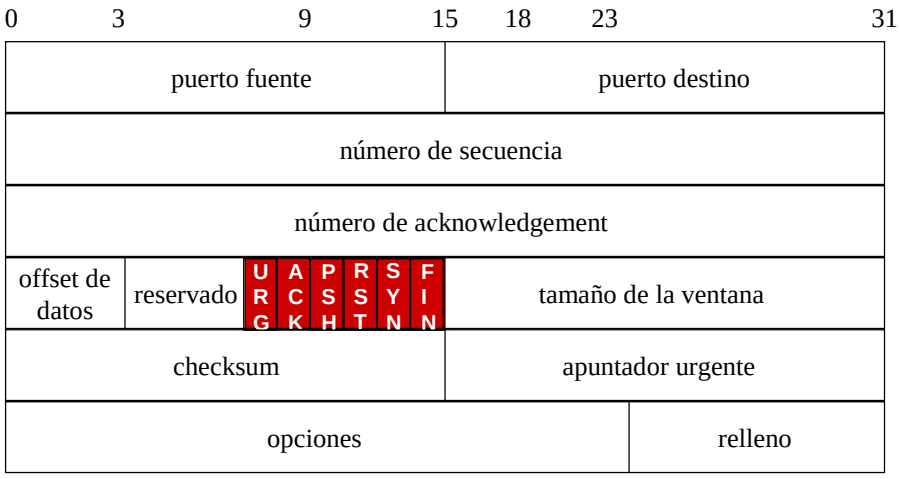


Lámina 20
Dr. Roberto Gómez C. (Seguridad en Redes)

Interpretación banderas TCP

- **SYN (Synchronization)**
  - Iniciar una conexión TCP
- **ACK (Acknowledgment)**
  - Indíca que el valor en el campo *número ack* es válido
- **FIN (Finish)**
  - Termina de forma "correcta" una conexión TCP
- **RST (Reset)**
  - Termina inmediatamente una conexión TCP
- **PSH (Push)**
  - Le indica al receptor pasar a los datos lo más rápido posible
- **URG (Urgent)**
  - Indica que el apuntador urgente es válido, generalmente causado por una interrupción

Lámina 21 Dr. Roberto Gómez C. (Seguridad en Redes)

Valores normales banderas

- **SYN, SYN ACK** y **ACK**
  - usados durante el three-way handshake
- **ACK**
  - a excepción paquete inicial SYN, cada paquete en una conexión debe tener el bit ACK activo
- **FIN ACK** y **ACK**
  - son usados para terminar una conexión existente
- **PSH FIN ACK**
  - también pueden ser vistos al principio de una deconexión
- **RST** o **RST ACK**
  - pueden usarse para terminar inmediatamente una conexión existente
- Paquetes durante "conversación" (despues handskake y antes deconexión) solo contienen un ACK por default
  - opcionalmente puede contenir **PSH** y/o **URG**

Lámina 22 Dr. Roberto Gómez C. (Seguridad en Redes)

Valores anormales

- **SYN FIN**
  - probablemente la combinación ilegal más conocida
- **SYN FIN PSH, SYN FIN RST, SYN FIN RST PSH**
  - y otras variantes de **SYN FIN** también existen
  - objetivo: evadir IDS que buscan paquetes con solo bits **SYN** y **FIN** activos
- Paquetes con solo la bandera **FIN** activa
  - paquetes usados para scaneos de puertos
- Paquetes sin ninguna bandera activa
  - paquetes conocidos como paquetes nulos

Lámina 23 Dr. Roberto Gómez C. (Seguridad en Redes)

Otros posibles valores anormales

- Paquetes nunca deben tener una dirección fuente o destino igual a 0
- El número de ack nunca debe tener un valor de 0 cuando la bandera ACK esta activa
- Un paquete con solo SYN activo no debe contener datos
  - lo anterior se da cuando una nueva conexión se inicia
- Paquetes no deben usar una dirección destino que sea una dirección de broadcast
  - usualmente terminan en .0 o .255
  - .0 es un viejo estilo de broadcast
- Normalmente no se realizan broadcasts usando TCP

Lámina 24 Dr. Roberto Gómez C. (Seguridad en Redes)

Ataques paquetes mal formados

Nombre	Funcionamiento	Plataformas vulnerables
Land	Envía paquetes con dirección IP y puerto destino/origen iguales	Sistemas Windows, varios Tipos Unix, impresoras, ruteadores
Latierra	Variante distribuida de Land	Sistemas Windows, varios Unix, ruteradores, impresoras
Ping de la muerte	Paquete ping grande	Windows, variantes Unix, impresoras
Jolt2	Envío paquetes fragmentados con valor de *fragment offset* NO cero	Windows 95, 98, NT y 2000
Teardrop, Newtear, Bonk, Syndrop	Herramientas que envían fragmentos de paquetes IP que se sobreponen, con valores tales que no se pueden reensamblar.	Windows 95, 98, NT y Linux
Winnuke	Envía basura a un puerto 139 TCP en una máquina Windows, afectando formateo SMB.	Windows 95 y NT

Lámina 25
Dr. Roberto Gómez C. (Seguridad en Redes)

Ejemplos ataques DoS

- Ping de la muerte
- Inundación Syn
- Spoofing
- Smurf
- Fraggle
- Fuga de memoria en Windows
- DoS Distribuido
- La herramienta Dsniff

Lámina 26
Dr. Roberto Gómez C. (Seguridad en Redes)

Ping de la muerte

- Ping sirve principalmente para saber si un servidor esta activo y poder calcular el trafico en la red según el tiempo de su respuesta.
  - básicamente se le envía un paquete a un servidor y este nos contesta,
- Si se envía un paquete muy grande puede llegar desordenado,
  - por lo que el servidor pide al origen que le vuelva a enviar una parte o la totalidad del paquete, por lo que se produce un datagrama del ping muy grande y producirá su caída.
- Para ejecutar este ataque se tiene que escribir :

```
c:\>ping -l 65510 victima.com
```

Lámina 27 Dr. Roberto Gómez C. (Seguridad en Redes)

Ping de la muertes y paquetes defragmentados.

- En lugar de enviar todo el paquete, se envía el paquete defragmentado.
- La víctima recibe el paquete y empieza a reensamblarlo.
- Sin embargo, debido al tamaño del paquete, una vez que este es reensamblado, es demasiado grande para el buffer y este se desborda.
- Lo anterior puede provocar resultados impredecibles
  - reinicializar la máquina (reboot)
  - suspender la máquina (hang)

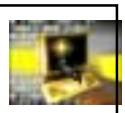
Lámina 28 Dr. Roberto Gómez C. (Seguridad en Redes)

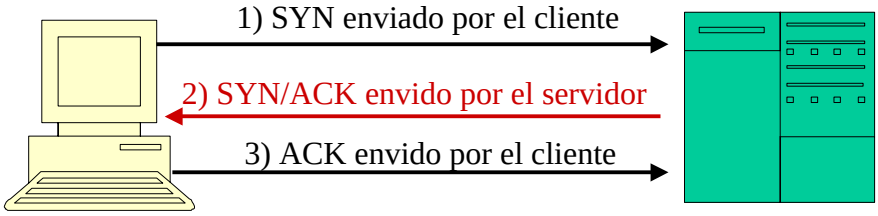
Inundación syn

- El ataque se basa en el mecanismo de establecimiento de una conexión TCP.
- El problema que explota es que cada sistema reserva una cantidad finita de recursos una vez ha envido el mensaje SYN/ACK para terminar el establecimiento de la conexión.
- El objetivo del atacante es abrumar la máquina destino con paquetes SYN.
  - cuado la victima recibe más paquetes SYN de los que puede manejar, otro tipo de tráfico no podrá llegar a la victima

Lámina 29 Dr. Roberto Gómez C. (Seguridad en Redes)

Conexión TCP normal





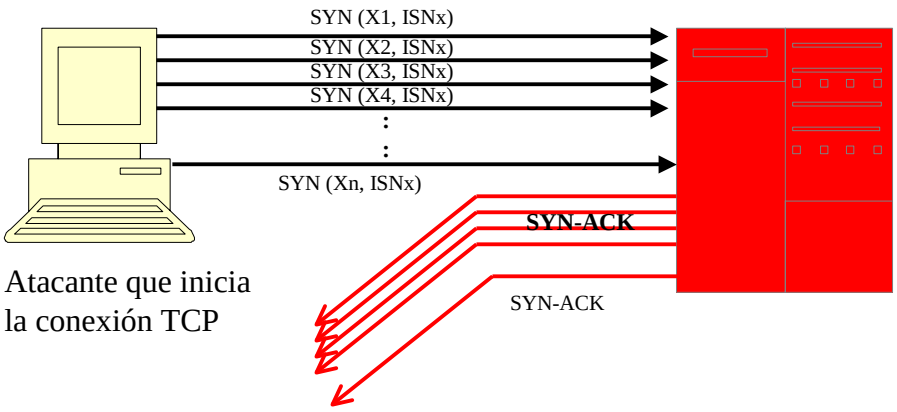
1. Paquete con el bit de bandera SYN activado
2. Para recordar numero secuencia inicial del origen, se reserva una cantidad de memoria en máquina destino. Se envía un syn/ack al cliente
3. El cliente envía un ack al servidor

Lámina 30 Dr. Roberto Gómez C. (Seguridad en Redes)

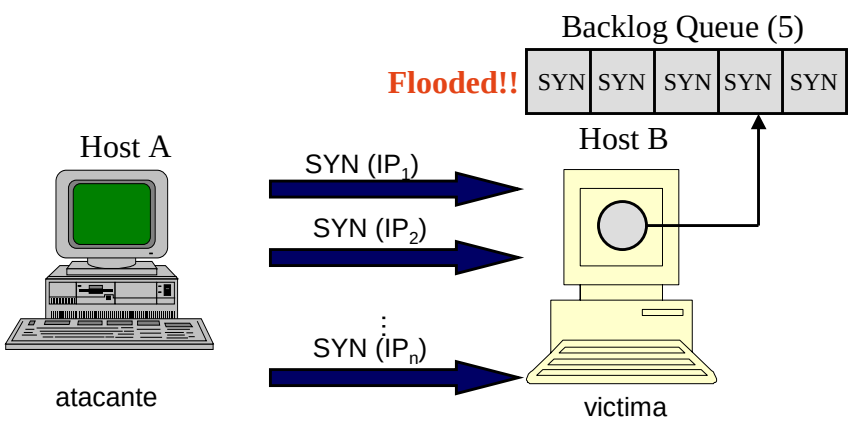
¿Y cómo se hace?

- Dos formas de hacerlo
- La primera inunda la cola de conexiones del sistema objetivo con medias conexiones abiertas
- La segunda es enviar paquetes syn de conexión con la dirección IP de otras máquinas.

Inundación syn



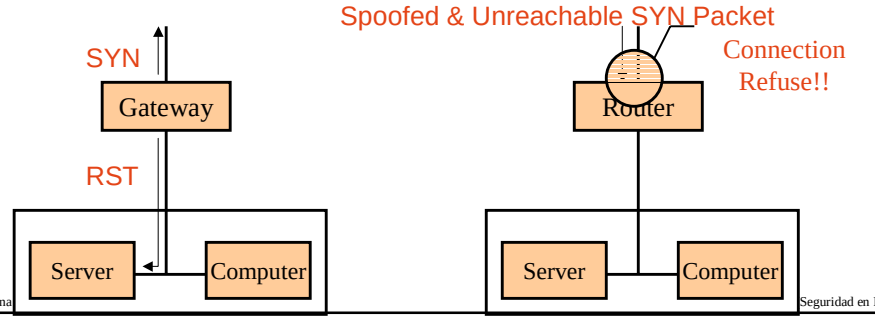
La segunda opción



SYN (IP_i): Son direcciones IP "spoofeadas" e inalcanzables

Contramedidas inundación syn

- Aumentar el tamaño de la cola de conexión
- Disminuir período tiempo establecimiento conexión
- Filtrado de paquetes
  - direcciones IP no "alcanzables"
- Emplear parches software de los fabricantes de los SO



Smurfing/Fraggle

- Ataque que afecta, principalmente, a la disponibilidad de los equipos.
- Se lleva a cabo principalmente en ruteadores Cisco y probablemente en otras marcas.
- Consiste en pedir una respuesta a varias máquinas y haciendose pasar por otra computadora.
  - de esta forma todas las respuestas llegaran a la víctima

Lámina 35 Dr. Roberto Gómez C. (Seguridad en Redes)

Smurfing

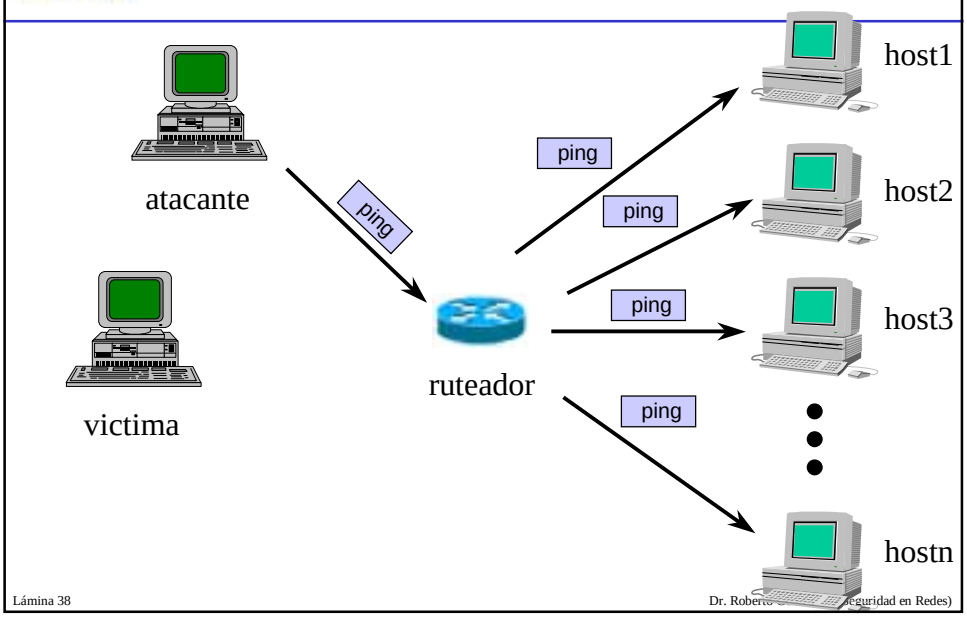
- Smurf es uno de los ataques de DoS más temidos.
- Requiere 3 actores: La víctima, el atacante y la red amplificadora
  1. El atacante originará un paquete ICMP hacia la dirección de broadcast de la red amplificadora, haciendo aparecer que su origen es una interfaz de la red de la víctima
  2. Cada interfaz de la red amplificadora enviará respuestas a la supuesta interfaz de origen

Lámina 36 Dr. Roberto Gómez C. (Seguridad en Redes)

Smurfing: Fraggle

- El objetivo y los actores son iguales que en un ataque smurf pero difiere en el tipo de paquete enviado
- Aquí se envía un paquete UDP al puerto 7 (echo) de todas las maquinas de la red amplificadora
- Si el puerto 7 está habilitado la estación responderá a la estación de origen
- Si el puerto 7 no está habilitado generará un mensaje ICMP “Puerto Inalcanzable”

El smurfing/fraggle 1/2



El smurfing/fraggle 2/2

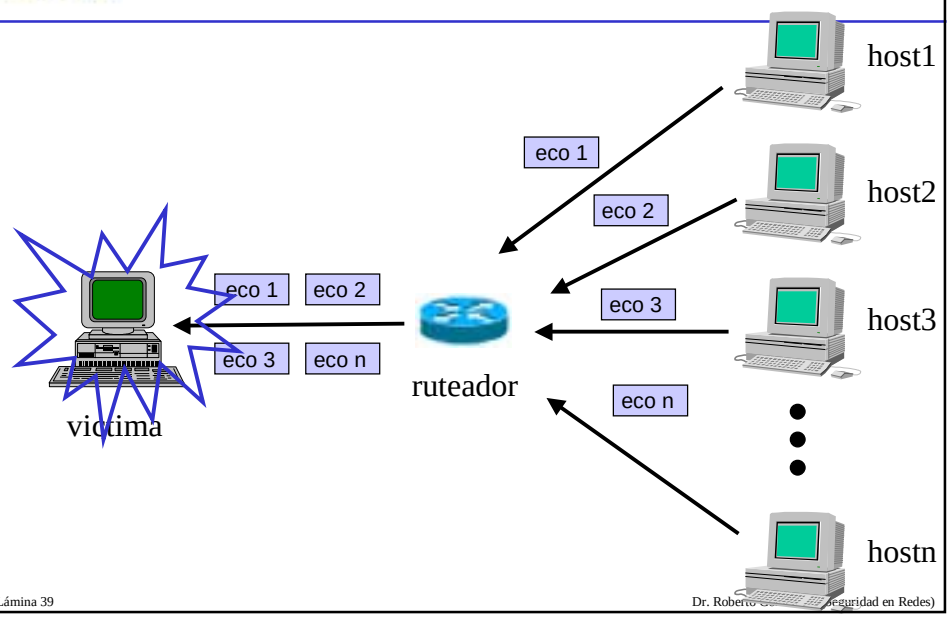


Lámina 39
Dr. Roberto G... (Seguridad en Redes)

Previniendo smurf/fraggle

- Para no permitir ser utilizado como red amplificadora debe deshabilitar el paso de mensajes destinados a broadcast a través de los routers de frontera
  - Cisco: no ip direct-broadcast
- Para limitar el daño ocurrido por un ataque de este tipo sobre su red, limite el tráfico ICMP a un valor razonable de acuerdo a su disponibilidad de ancho de banda
- Verifique si realmente necesita permitir tráfico de entrada ICMP a toda su red

Lámina 40
Dr. Roberto Gómez C. (Seguridad en Redes)

DoDS: Negación Servicio Distribuido

- En febrero/marzo del 2000, varias empresas que apoyan su estrategia en Internet fueron atacadas.
  - Yahoo! estima pérdidas por US$500,000 dls por dejar de dar servicio durante 3 horas
- Entre ellas destacan:
  - CNN (Agencia Noticiosa)
  - Amazon (Venta de libros, discos, etc.)
  - e-Bay (Venta de artículos en remate)
  - e-Trade (compra y venta de acciones)
  - Yahoo (Correo gratuito)

Lámina 41 Dr. Roberto Gómez C. (Seguridad en Redes)

Descripción ataque sufrido

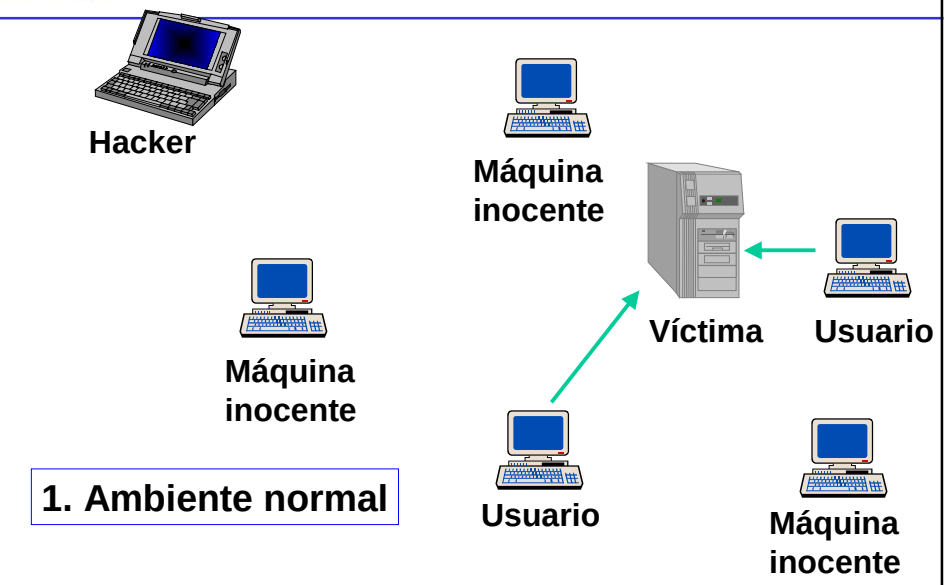
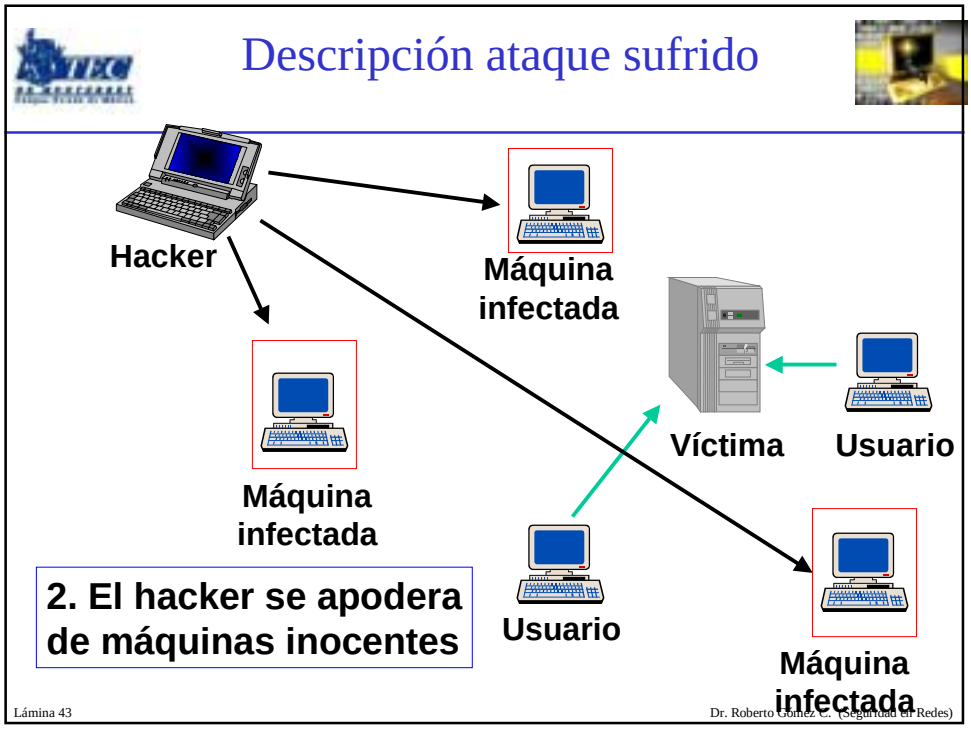
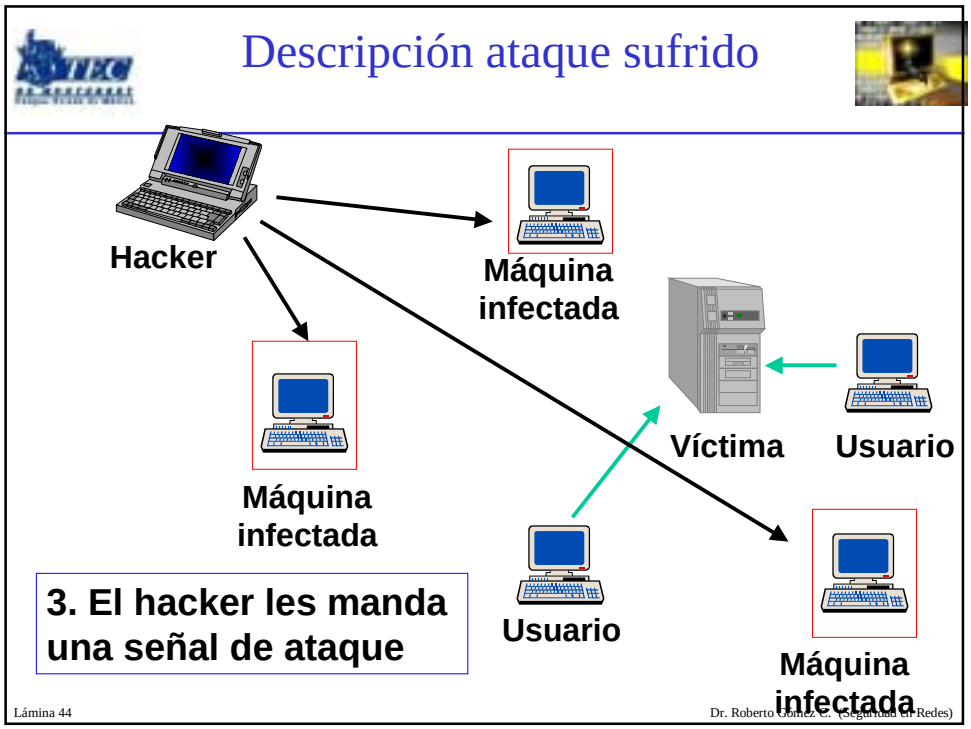
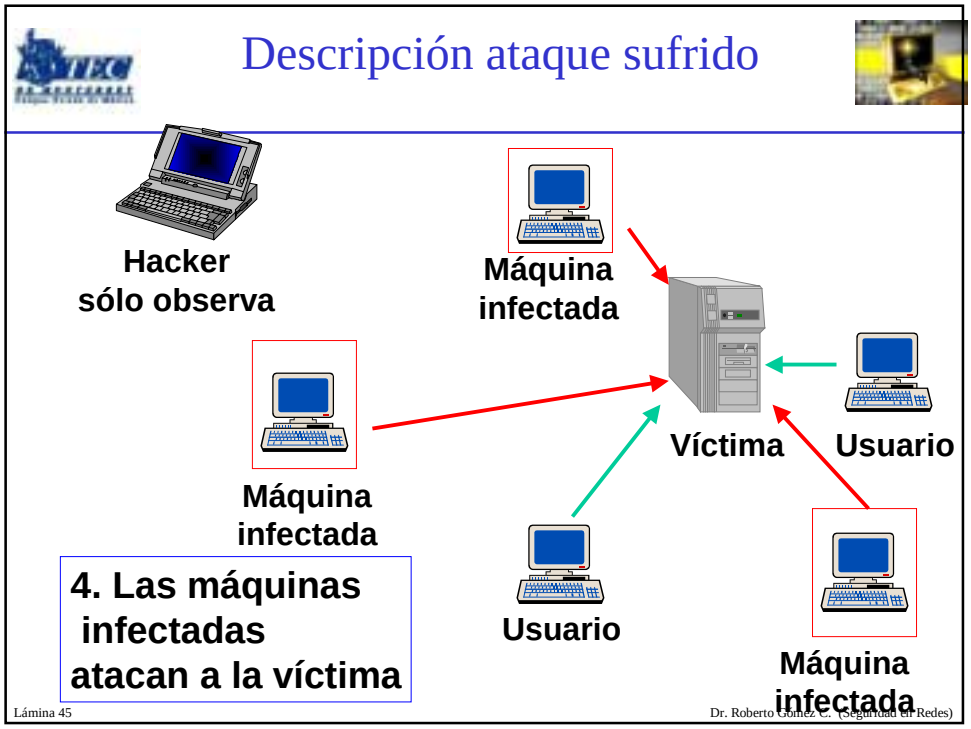
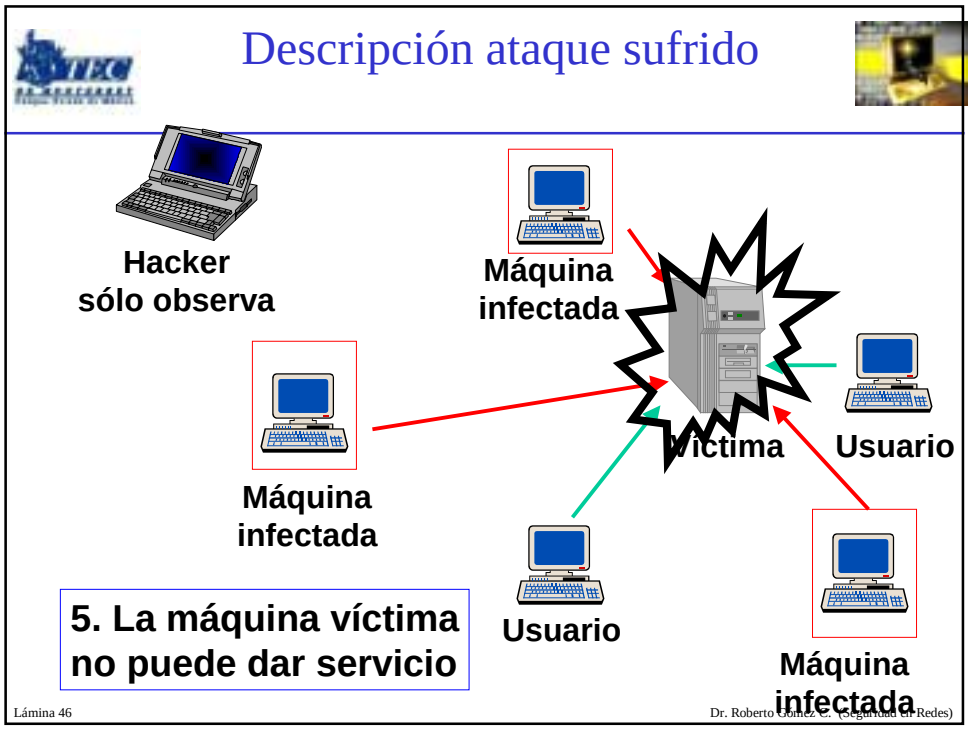


Lámina 42 Dr. Roberto Gómez C. (Seguridad en Redes)


Descripción ataque sufrido
Hacker
Máquina infectada
Máquina infectada
Víctima
Usuario
Usuario
Máquina infectada
2. El hacker se apodera de máquinas inocentes
Lámina 43
Dr. Roberto Gómez C. (Seguridad en Redes)


Descripción ataque sufrido
Hacker
Máquina infectada
Máquina infectada
Víctima
Usuario
Usuario
Máquina infectada
3. El hacker les manda una señal de ataque
Lámina 44
Dr. Roberto Gómez C. (Seguridad en Redes)


Descripción ataque sufrido
Hacker
sólo observa
Máquina
infectada
Víctima
Usuario
Máquina
infectada
Usuario
Máquina
infectada
4. Las máquinas infectadas atacan a la víctima
Lámina 45
Dr. Roberto Gómez C. (Seguridad en Redes)


Descripción ataque sufrido
Hacker
sólo observa
Máquina
infectada
Víctima
Usuario
Máquina
infectada
Usuario
Máquina
infectada
5. La máquina víctima no puede dar servicio
Lámina 46
Dr. Roberto Gómez C. (Seguridad en Redes)


Mission: Total Overload
Hacker
The Web
Network
'I'm here'


No me van a creer, pero acabo de recibir por parte de mi esposa un ATAQUE DE NEGACIÓN DE SERVICIO
A la moda...
por jamaya
Lámina 48
Dr. Roberto Gómez C. (Seguridad en Redes)

¿Y cómo creo un paquete mal formado?

- Programas inyectores de paquetes
- Objetivo
  - formar sus propios paquetes de red e inyectarlos en la red
- Diferentes tipos de protocolos soportados
- Diferentes tipos de red soportadas
- En un principio usados para probar firewalls, detectores de instrusos y servidores.

Paquetes Inyectores

- Send IP
  - http://www.earth.li/projectpurple/progs/sendip.html
  - herramienta de comando línea que permite enviar paquetes IP arbitrarios
- wINJECT:
  - inyección de paquetes para Win9x & Win2k
  - home19.inet.tele.dk/moofz/about_o.htm
- Nemesis (packet injection)
  - inyección de paquetes de comando de línea Unix
  - http://www.packetfactory.net/Projects/nemesis

Características SendIP

- Cuenta con un gran número de opciones de comando de línea para especificar cada el contenido del encabezado de NTP, BGP, RIP, TCP, UDP, ICMP o paquetes raw IPv4 e IPv6
  - también permite añadir cualquier dato a los paquetes
- Ultima versión: 2.1, 24/02/2002
- Documentación
  - incluye un manpage, así como un archivo README
  - el código fuente es bastante legible ;)
- Licencia
  - distribuido de acuerdo a la licencia pública GNU
  - fue escrito por Mike Ricketts.

Lámina 51 Dr. Roberto Gómez C. (Seguridad en Redes)

Características wINJECT

- Construye todos los paquetes posibles e imposibles
  - TCP/IP
  - ICMP
  - UDP
  - los de costumbre
  - otros? más? tan solo hay que crearlos !!!!
- Hex Dump de un paquete para su mejor análisis
- Spoof Source IP.
- Random Source IP.
- Dynamic IP insert.

Lámina 52 Dr. Roberto Gómez C. (Seguridad en Redes)

Nemesis

- Software de inserción de paquetes, que soporta
  - ARP, DNS, ICMP, IGMP. OSPF. RARP. RIP. TCP, UDP
- Desarrollado por Mark Grimes (obecian@packetninja.net, obecian@openbsd.org)
- Libnet-based (extremely portbale) – *BSD, Solaris, MacOSx, Linux
- Node Integrity/Evasion Testing (Router/Switch/Firewall/IDS/Stack)
- Router Congestion Management
- Covert Channels, Spoofing, Evasion

Requerimientos

- Para compilarlo y correrlo es necesario contar con Libnet y Libpcap
  - libnet:http://www.packetfactory.net/Projects/Libnet/
  - libpcap: http://www.tcpdump.org/
- Usuarios Solaris
  - autor indica que le tomo un poco de tiempo (few hours) de manejar Libpcap incluyendo archivos de viejas versiones del paquete
  - posible que lo mismo ocurra con nuevas versiones de núcleos de Linux

Características particulares

- Ofrece características nuevas que no se pueden encontrar en ninguna otra herramienta de su clase.
- Inyección de paquetes puede ser controlada a nivel capa 2 o capa 3 (como el protocolo lo permita)
  - importante en el mundo de los nuevos productos Cisco
  - se tienen reportes del uso “out-of-band” tcp/udp en capa 2 (en lugar de la usual capa 3)
- Unica herramienta de stack ip que ofrece los dos protocolos de ruteo: dynamic vector (RIP) y link state (OSPF)
  - paquetes OSPF son raramente no explorados

Lámina 55 Dr. Roberto Gómez C. (Seguridad en Redes)

Ejemplos nemesis

- nemesis-tcp -v -S 192.168.1.1 -D 192.168.2.2 -fS -fA -y 22 -P toto
  - envía paquete TCP (SYN/ACK) con payload del archivo ascii *toto* al puerto ssh, de 192.168.1.1 a 192.168.2.2
  - opción –v permite visualizar el paquete inyectado
- nemesis-udp -v -S 10.11.12.13 -D 10.1.1.2 -x 11111 -y 53 -P bindpkt
  - envia paquete UDP de 10.11.12.13:11111 al puerto de servicio de nombres de 10.1.1.2, con un payload que se lee del archivo *bindpkt*
  - de nuevo: -v usado para confirmar paquete inyectado
- nemesis-icmp -S 10.10.10.3 -D 10.10.10.1 -G 10.10.10.3 -i 5
  - enviar paquete ICMP REDIRECT de 10.10.10.3 a 10.10.10.1 con la dirección del gateway como dirección fuente

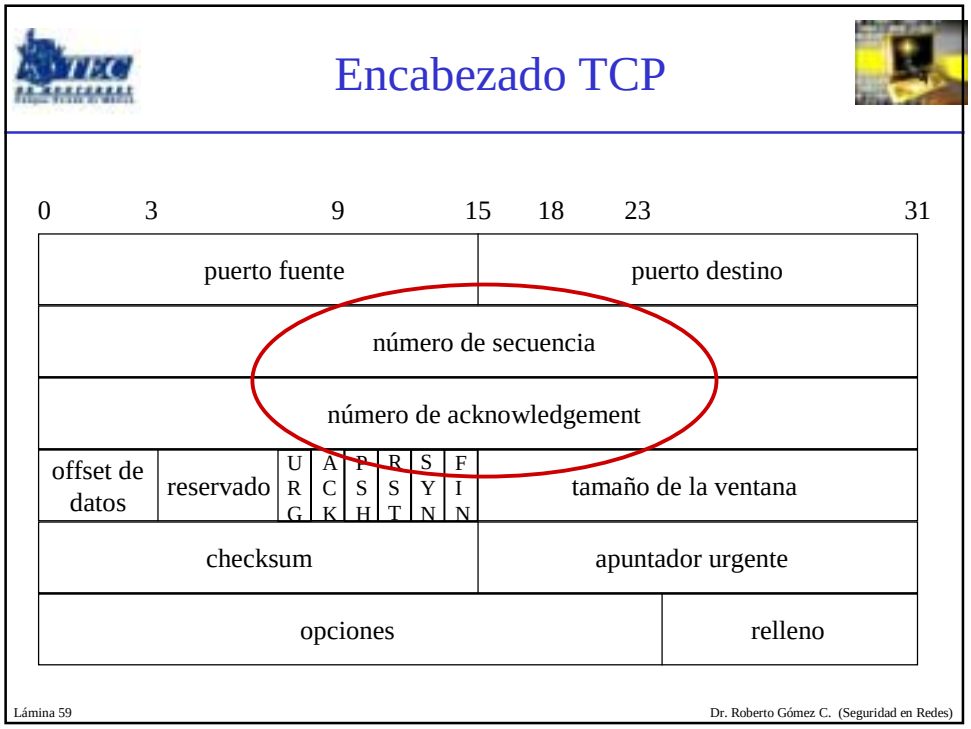
Lámina 56 Dr. Roberto Gómez C. (Seguridad en Redes)

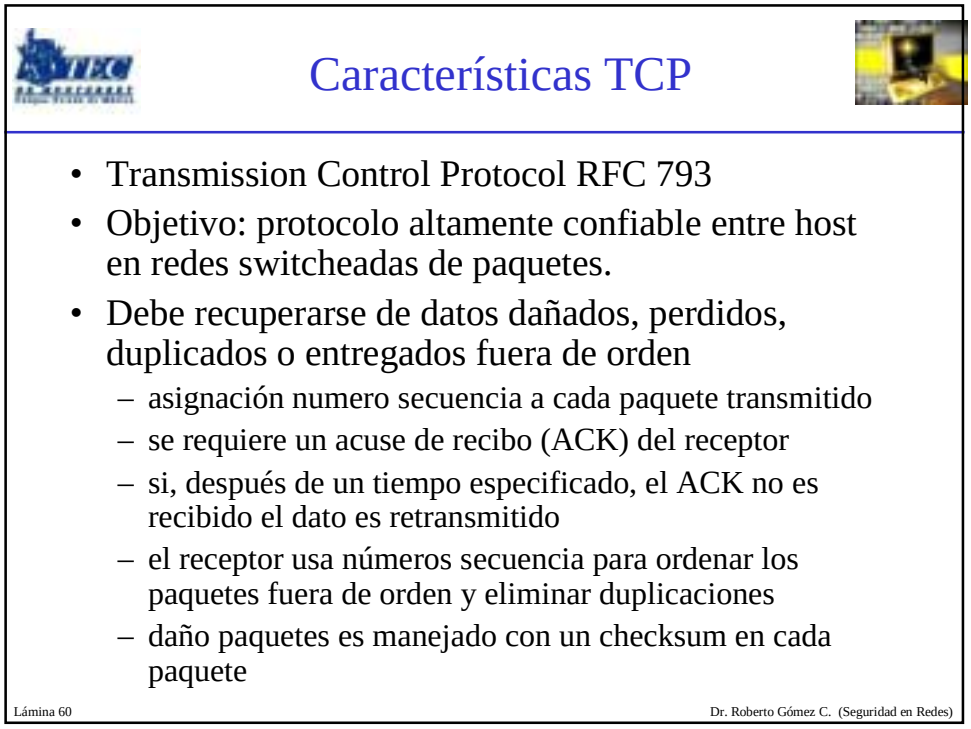
Otro software relacionado

- Arp Inject 0.1
- Snot 0.8.5
- TCP Kill
- "Multi-Generator" (MGEN) Toolset
- isic
- rid-1.11

Secuestro de sesiones

- Termino en inglés: hijacking
- Tipo de ataque en el que el atacante toma control de una comunicación tal y como un secuestrador de aviones tomo control del avión.
  - entre dos entidades y haciendo pasar por una de ellas
- En un tipo de ataque (man in the middle)
  - el atacante toma control de la conexión mientras esta se produce.
- El objetivo es robar una conexión generada por un aplicación de red iniciada por un cliente (p.e. telnet)
  - conseguir un programa en Internet
  - hacerlo manualmente


Encabezado TCP
0
3
9
15
18
23
31
puerto fuente
puerto destino
número de secuencia
número de acknowledgement
offset de datos
reservado
URG
ACK
PSH
RST
SYN
FIN
tamaño de la ventana
checksum
apuntador urgente
opciones
relleno
Lámina 59
Dr. Roberto Gómez C. (Seguridad en Redes)


Características TCP
• Transmission Control Protocol RFC 793
• Objetivo: protocolo altamente confiable entre host en redes switcheadas de paquetes.
• Debe recuperarse de datos dañados, perdidos, duplicados o entregados fuera de orden
– asignación numero secuencia a cada paquete transmitido
– se requiere un acuse de recibo (ACK) del receptor
– si, después de un tiempo especificado, el ACK no es recibido el dato es retransmitido
– el receptor usa números secuencia para ordenar los paquetes fuera de orden y eliminar duplicaciones
– daño paquetes es manejado con un checksum en cada paquete
Lámina 60
Dr. Roberto Gómez C. (Seguridad en Redes)

El numero de secuencia

- Cada paquete de datos enviado a través de una conexión TCP tiene un número de secuencia.
  - se tienen acuse recibo por cada paquete
- Sistema acuse recibo es acumulativo
  - el ack del numero secuencia X, indica que todos los paquetes hasta, pero incluyendo, X se han recibido
- Numeración es en base a los bytes del paquete
  - cada byte tiene un número de secuencia
  - primer dato que sigue al encabezado tiene el menor valor
  - los siguientes bytes son numerados secuencialmente
  - espacio numeración finito pero grande (0 a $2^{32} - 1$)

Lámina 61 Dr. Roberto Gómez C. (Seguridad en Redes)

El ataque

- La predicción de secuencia en una red fue escrito por primera vez en 1985
  - Robert T. Morris (su hijo creo el gusano del 88)
- Primer ataque usando esta técnica se dio hasta la navidad de 1994
  - conocido como Mitnick hack of Shimomura (o Christmas Hack)

Lámina 62 Dr. Roberto Gómez C. (Seguridad en Redes)

Secuestrando sesión telnet

- Campo SEQ: Los datos de este campo son usados para definir la secuencia de los paquetes enviados.
  - esta en hexadecimal y el servidor pondrá estos datos en el campo ACK del paquete que envíe al cliente
- El hijacking es básicamente predecir los datos de los campos SEQ y ACK para enviar paquetes falsos que serán aceptados por el servidor sin que note nada anormal.

Lámina 63 Dr. Roberto Gómez C. (Seguridad en Redes)

Principios del ataque

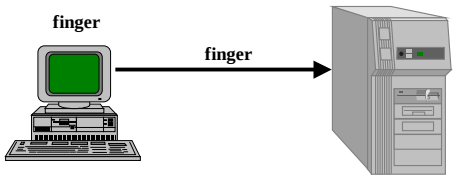
- Una vez que el numero de secuencia se ha establecido
  - todos los datos serán ISN + 1
- El truco no esta en secuestrar la sesión
  - encontrar el ISN
- Tres requerimientos para secuestrar comunicación TCP
  - tráfico no debe estar encriptado
  - atacante debe ser capaz de reconocer los números de secuencia TCP y predecir el número siguiente
  - atacante debe “spoofear” direcciones MAC e IP para recibir comunicaciones no dirigidas a él.

Lámina 64 Dr. Roberto Gómez C. (Seguridad en Redes)

Esquema secuestro (1/4)

Cliente → Servidor

* SEQ: Los datos de este campo son usados para definir la secuencia de los paquetes enviados. Esta en hexadecimal y el server lo que hara con estos datos es ponerlos en el campo ACK del paquete que envie al cliente.



195.1.1.1
Maquina cliente

servidor
194.1.1.1

máquina Hijacker
195.1.1.3

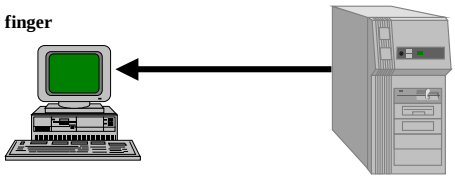
TCP paquet ID ->IP-Cliente.puerto:195.1.1.1.1025->IP-Server.puerto:194.1.1.1.23
***SEQ ----------> 3DF454DA**
****ACK ----------> F454FDF5**
Flag ----------> -AP---
Paquet ID ----->IP-Cliente.puerto:195.1.1.1.1025->IP-Server.puerto:194.1.1.1.23
DATA ----------> AE 00) 33 GF (bla ,bla, bla AE 00)

Lámina 65
Dr. Roberto Gómez C. (Seguridad en Redes)

Esquema secuestro (2/4)

Servidor → Cliente

El servidor, traduce el contenido del paquete, y lo ejecuta, escribiendo la "f" en la shell, y envia otro paquete al cliente, que en realidad es un "echo" del recibido por el cliente para que el cliente se cerciore de que el paquete ha llegado y ha sido ejecutado



195.1.1.1
Maquina cliente

servidor
194.1.1.1

***SEQ ----------> 3DF454DA**
****ACK ----------> F454FDF5**
Flag ----------> -AP---

máquina Hijacker
195.1.1.3

TCP paquet ID-> IP-Server.puerto:194.1.1.1.23-> IP Cliente.puerto:195.1.1.1.1025
SEQ ----------> F454FDF5
ACK ----------> 3DF454E4
Flags ----------> -AP---
Paquet ID ----> IP-Server.puerto:194.1.1.1.23-> IP-Cliente.puerto:195.1.1.1.1025
DATA ----------> AE 00) 33 GF (bla ,bla, bla)

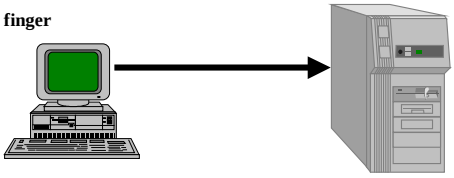
Lámina 66
Dr. Roberto Gómez C. (Seguridad en Redes)

Esquema secuestro (3/4)

Cliente → Servidor

El cliente enviara un paquete ACK, como respuesta al paquete que acaba de enviar el servidor, este paquete no contendra DATA. Solo sirve para confirmar que ha llegado el paquete del servidor.

finger



195.1.1.1
Maquina cliente

servidor
194.1.1.1

máquina Hijacker
195.1.1.3

TCP paquet ID->IP-Cliente.puerto:195.1.1.1.1025->IP-Server.puerto:194.1.1.1.23
SEQ ----------> 3DF454E4
ACK ----------> F454FDFF
Flag ----------> -A----
Paquet ID ---->IP-Cliente.puerto:195.1.1.1.1025->IP-Server.puerto:194.1.1.1.23
DATA ----------> (2 bytes de data, que no tienen valor)

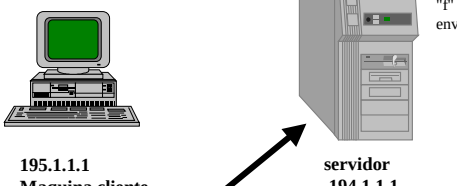
Lámina 67
Dr. Roberto Gómez C. (Seguridad en Redes)

Esquema secuestro (4/4)

Hijacker → Servidor

Ahora es cuando debemos enviar nuevos datos al servidor haciendonos pasar por el Cliente. Para lograrlo debemos calcular la secuencia del paquete "spoofed" que enviaremos de los numeros SEQ y ACK, basandonos en el primer paquete que hemos interceptado (¿sniffado? :-?). Debemos enviar datos al servidor para que no se ejecute el comando que el cliente estaba introduciondo (que por ahora solo habia enviado la "f" del "finger", con lo cual sea mas facil), para que esto ocurra enviamos retornos de carro, o lo que nos plazca.

finger



195.1.1.1
Maquina cliente

servidor
194.1.1.1

máquina Hijacker
195.1.1.3

TCP paquet ID->IP-Cliente.puerto:195.1.1.1.1025->IP-Server.puerto:194.1.1.1.23
SEQ ----------> 3DF454E4
******ACK ----------> F454FE09**
Flag ----------> -AP---
Paquet ID ---->IP-Cliente.puerto:195.1.1.1.1025->IP-Server.puerto:194.1.1.1.23
DATA ----------> AE 00) 33 GF (bla ,bla, bla)
****** ACK ---------> F454FE09 = F454FDFF + 0A.**

Lámina 68
Dr. Roberto Gómez C. (Seguridad en Redes)

Enviando más paquetes

- Es posible enviar cuantos paquetes se desee,
  - puesto que se conoce como falsearlos.
- La cantidad que se le suma al número que se recibió (SEQ), para meterlo en campo ACK es el tamaño de los datos, del paquete que se va a enviar.
- Ejemplo:
  - se interceptó el paquete que servidor envio al cliente en paso 2
  - lo que mas interesa es el numero del campo SEQ , F454FDF5,
  - despues el Cliente envio un paquete ACK, con el numero F454FDFF, que es el F454FDF5 + el tamaño de los datos que en hexadecimal es 0A,
  - por ultimo el Hijacker envía un paquete con el ACK F454FDFF + el tamaño de los datos, que tambien es 0A.

Lámina 69 Dr. Roberto Gómez C. (Seguridad en Redes)

¿Y el cliente original?

- Una vez que se logra predecir la secuencia de números del SEQ/ACK se puede enviar los comandos que se desee sin preocupación.
- El cliente no recibirá nada
  - creerá que se le ha colgado la conexión, como suele pasar a veces sin necesidad de ningún hacker de por medio.

Lámina 70 Dr. Roberto Gómez C. (Seguridad en Redes)

La herramienta Hunt

- Desarrollado por Pavel Krauz
- Versión actual: 1.5
- Programa para introducirse en una conexión tcp, verla y resetearla
- Requiere Linux 2.2, GlibC 2.1 con LinuxThreads, Ethernet.
- Cuenta con engines de paquetes para ver tráfico TCP, ICMP y tráfico ARP, colectando conexiones TCP con números de secuencia.
- Ambientes switcheados
  - hosts en puertos switched pueden ser spoofeados, sniffeados y secuestrados

Lámina 71
Dr. Roberto Gómez C. (Seguridad en Redes)

Hunt funcionando

```
/*
 *      hunt 1.5
 *      multipurpose connection intruder / sniffer for Linux
 *      (c) 1998-2000 by kra
 */
starting hunt
--- Main Menu --- rcvpkt 0, free/alloc 63/64 ------
l/w/r) list/watch/reset connections
u)     host up tests
a)     arp/simple hijack (avoids ack storm if arp used)
s)     simple hijack
d)     daemons rst/arp/sniff/mac
o)     options
x)     exit
->
```

```
0) 192.168.0.1 [1027]     --> 192.168.0.2 [23]
l/w/r) list/watch/reset connections
u)     host up tests
a)     arp/simple hijack (avoids ack storm if arp used)
s)     simple hijack
d)     daemons rst/arp/sniff/mac
o)     options
x)     exit
->
```

Lámina 72

Hunt secuestra una sesión

```
-> a
0) 192.168.0.1 [1027]          --> 192.168.0.2 [23]

choose conn> 0
arp spoof src in dst y/n [y]> y
src MAC [EA:1A:DE:AD:BE:01]> EA:1A:DE:AD:BE:02
arp spoof dst in src y/n [y]> y
dst MAC [EA:1A:DE:AD:BE:02]> EA:1A:DE:AD:BE:03
input mode [r]aw, [l]ine+echo+\r, line+[e]cho [r]> l
dump connectin y/n [y]> n
press key to take over of connection
```

```
press key to take over of connection
you took over the connection
CTRL-] to break
```

Lámina 73 Dr. Roberto Gómez C. (Seguridad en Redes)

Análisis de tráfico

- Termino en inglés: Traffic Analysis
- El análisis de trafico es una técnica complicada para inferir posibles sucesos a partir de la cantidad de información que circula en uno o varios segmentos de red.
- No es necesario que la información circule “en claro”.
- Usada por los americanos durante el inicio de la segunda guerra mundial

Lámina 74 Dr. Roberto Gómez C. (Seguridad en Redes)

Replay Attacks

- Alicia autoriza una transferencia de fondos de una cuenta a otra
  - encripta la petición de transferencia con una llave de firma que solo ella conoce
  - envía petición a una máquina que verifica la firma y lleva a cabo la transacción
- Un intruso, Eva, desea contar con la misma transacción repetida sin la autorización de Ana
  - no necesita producir la petición encriptada por ella misma
  - asumiendo que puede adivinar o deducir que mensaje corresponde a la transferencia solo necesita tomar el mensaje y enviarlo después

Lámina 75 Dr. Roberto Gómez C. (Seguridad en Redes)

Generalizando

- En general se asume “replay”
  - capturar un mensaje o una parte de un mensaje que es usado tiempo después
- Esto incluye los dos casos
  - el mensaje pasa sin impedimento alguno
  - el mensaje es verificado para que pueda pasar
- Es bueno preocuparse por este tipo de ataques.
  - aparte de contar con un buen algoritmo de encripción

Lámina 76 Dr. Roberto Gómez C. (Seguridad en Redes)