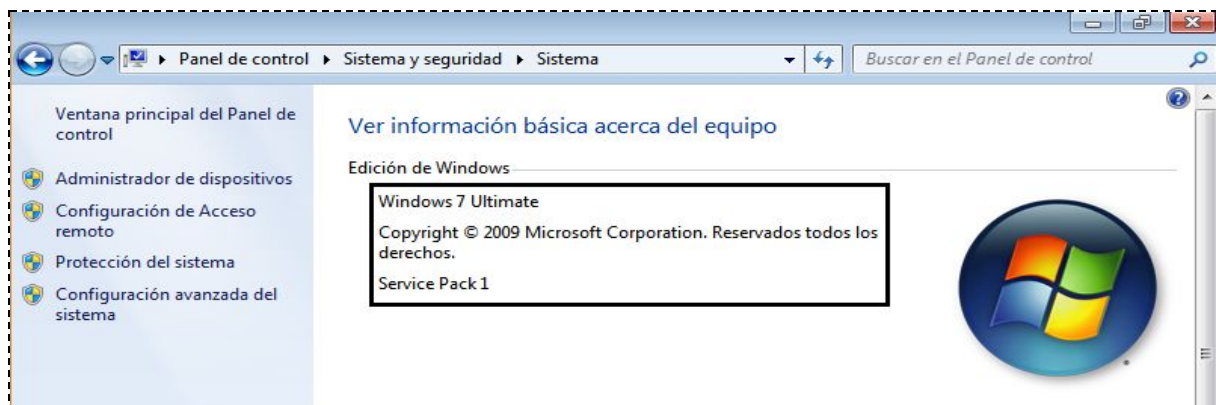


Caso Práctico

Christian Andrades Molina

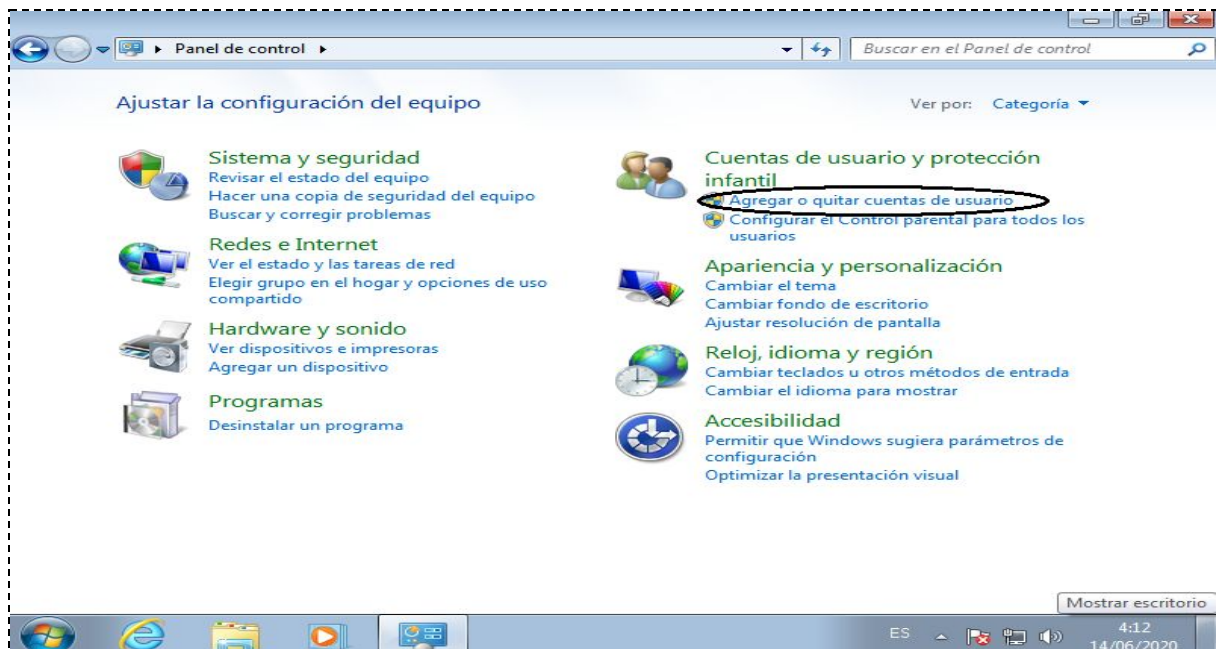
1. Lo primero que debemos realizar es obtener los datos de nuestro sistema operativo. Dependiendo del que usemos (Windows, Linux, Mac) tendremos una forma de sacar esa información.

La práctica está realizada sobre Windows 7 Ultimate en una máquina virtual mediante Oracle VM VirtualBox. Accediendo al *Panel de Control -> Sistema y seguridad -> Sistema* obtenemos la información del SO y el PC.

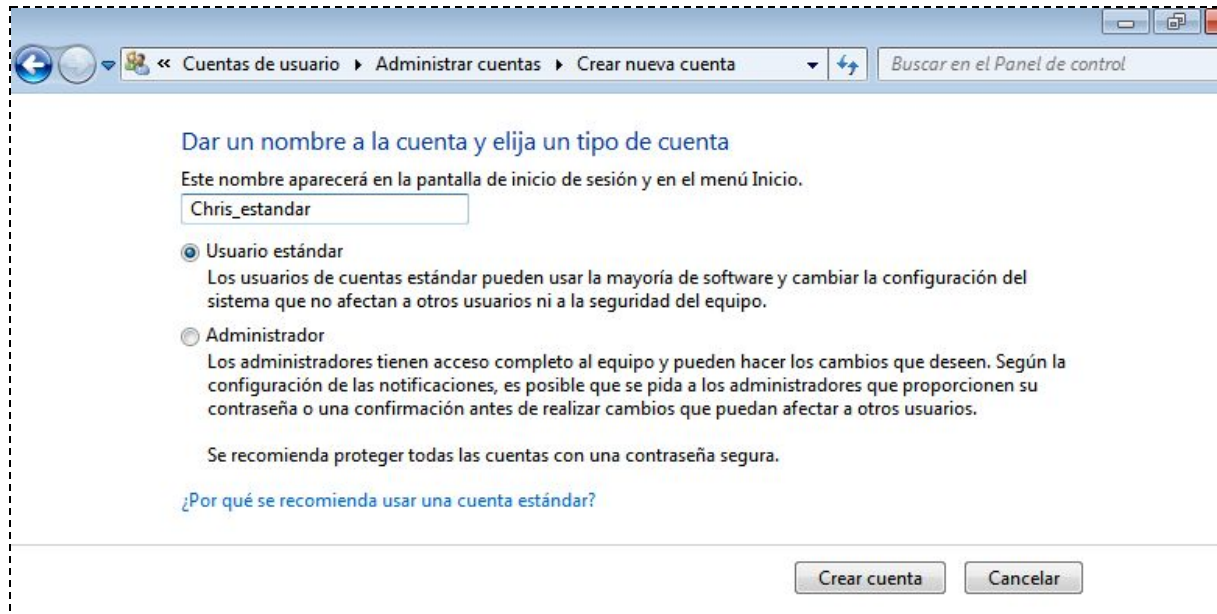


2. Lo siguiente es crear un usuario que NO sea administrador (ni invitado). Tanto el nombre como la contraseña lo dejo a vuestra elección.

Nos dirigimos al Panel de Control y cuentas de Usuario seleccionamos “Agregar cuentas de usuario”



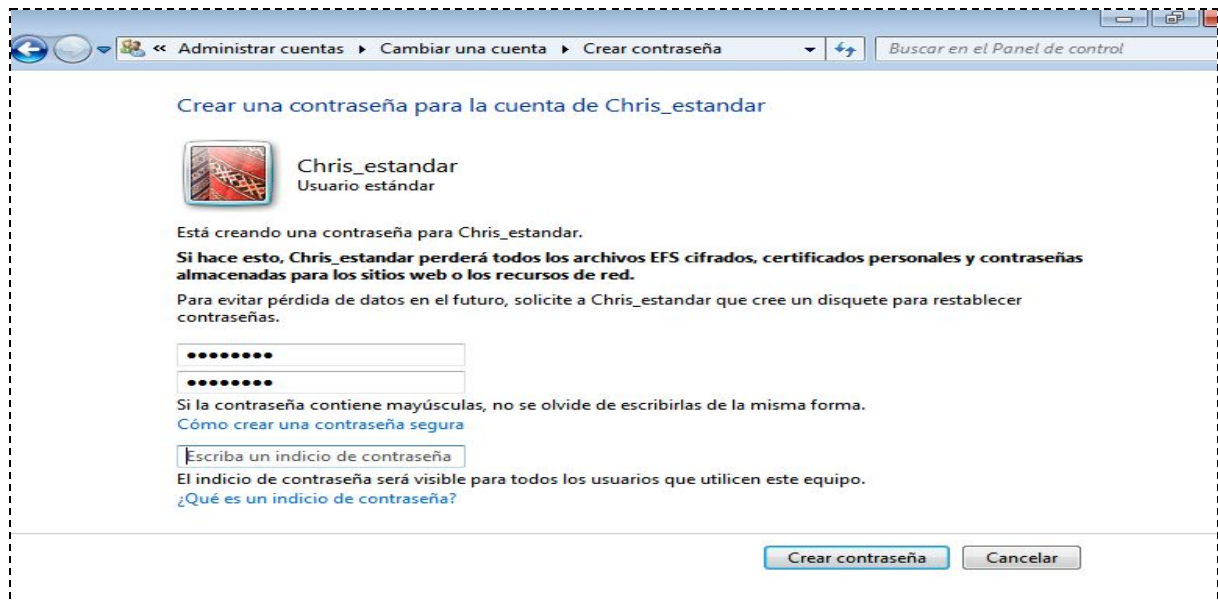
Damos un nombre a la nueva cuenta (usuario estándar).



Accedemos a la gestión de la nueva cuenta creada y seleccionamos "Crear una contraseña".



A la nueva cuenta le asociamos una contraseña que introducimos en dos ocasiones además de un indicio de la misma en caso de pérdida



3. Ahora accedemos al sistema operativo con ese usuario e intentamos instalar el siguiente programa:

a. Si usas Windows o Mac: Malwarebytes Anti-Malware.1

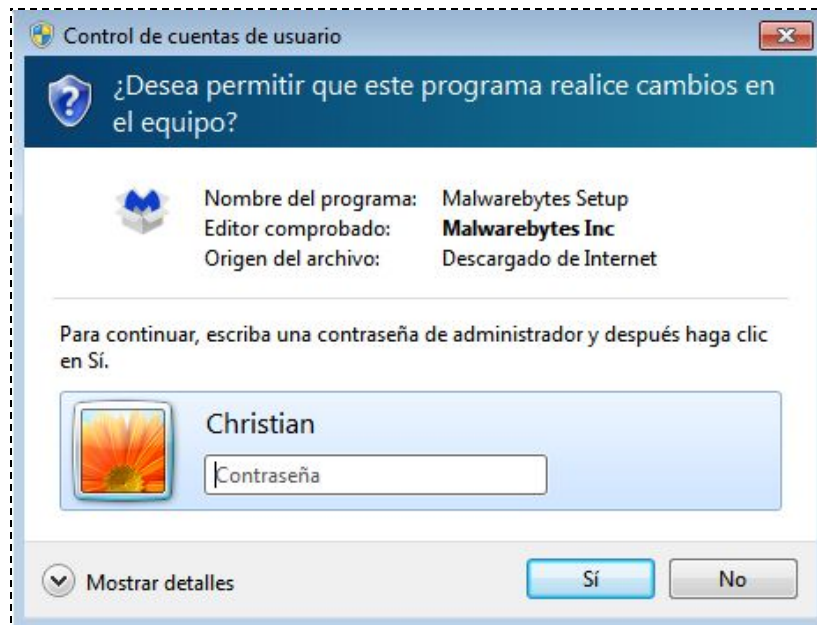
b. Si usas Linux: ClamAV

Tienes que sacar una captura de pantalla con lo que ocurre al intentar instalarlo.

Cerramos sesión con la cuenta actual y accedemos a la nueva estandar creada:



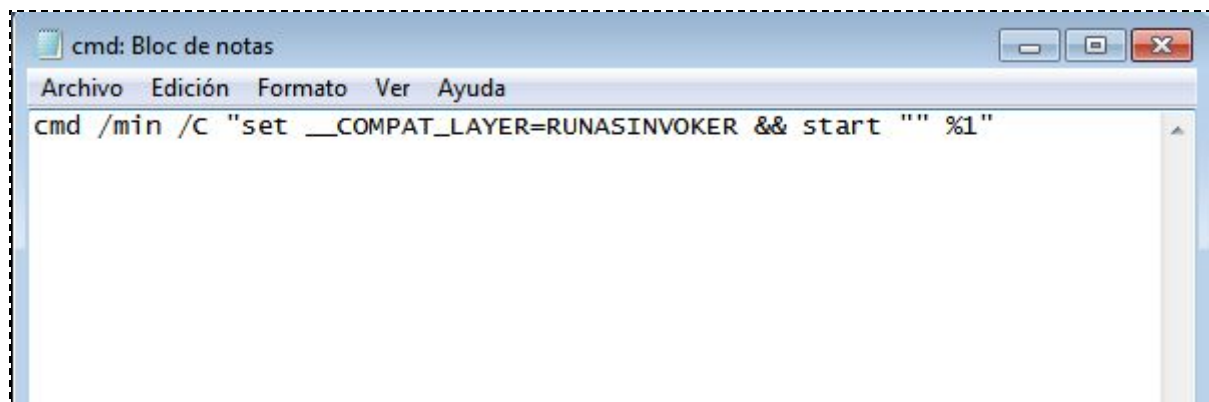
Al intentar instalarlo nos solicita la contraseña de la cuenta con funciones de administrador:



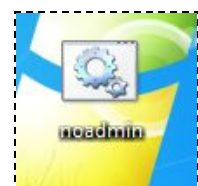
4. Instalar correctamente el programa e indicar cómo lo has hecho para solucionar el “problema” del paso anterior. NO se puede cambiar de cuenta. La idea es realizar la práctica entera con la cuenta recién creada.

Si conocemos la contraseña de la cuenta administrador podemos introducirla y acceder a la instalación sin ningún problema. Si no conocemos esta contraseña, existe una alternativa:

1. Creamos un nuevo archivo de texto con la siguiente línea de contenido:



2. En Archivo -> Guardar como ... marcamos como tipo “Todos los archivos” y guardamos el archivo.



3. Arrastramos el archivo de instalación hacia el fichero creado:



4. Y accedemos directamente a los pasos de instalación sin introducir la contraseña de administrador.



5. Realiza un escaneo rápido de tu equipo y muestra el resultado (siempre desde la cuenta creada en el paso 2).

Este es el resultado generado:

Malwarebytes
www.malwarebytes.com

-Detalles del registro-
Fecha del análisis: 14/6/20
Hora del análisis: 14:36

Archivo de registro: a90ac4b6-ae3b-11ea-9521-0800278cfce5.json

-Información del software-

Versión: 4.1.0.56

Versión de los componentes: 1.0.931

Versión del paquete de actualización: 1.0.25472

Licencia: Prueba

-Información del sistema-

SO: Windows 7 Service Pack 1

CPU: x64

Sistema de archivos: NTFS

Usuario: Christian-PC\Chris_estandar

-Resumen del análisis-

Tipo de análisis: Análisis de amenazas

Análisis iniciado por:: Manual

Resultado: Completado

Objetos analizados: 226327

Amenazas detectadas: 4

Amenazas en cuarentena: 0

Tiempo transcurrido: 0 min, 59 seg

-Opciones de análisis-

Memoria: Activado

Inicio: Activado

Sistema de archivos: Activado

Archivo: Activado

Rootkits: Desactivado

Heurística: Activado

PUP: Detectar

PUM: Detectar

-Detalles del análisis-

Proceso: 0

(No hay elementos maliciosos detectados)

Módulo: 0

(No hay elementos maliciosos detectados)

Clave del registro: 0

(No hay elementos maliciosos detectados)

Valor del registro: 4

PUM.Optional.DisableMRT, HKLM\SOFTWARE\POLICIES\MICROSOFT\MRT\DONTOFFERTHROUGHWUAU, Sin acciones por parte del usuario, 6916, 676880, 1.0.25472, , ame,

PUM.Optional.DisableMRT,

HKLM\SOFTWARE\POLICIES\MICROSOFT\MRT\DONTREPORTINFECTIONINFORMATION, Sin acciones por parte del usuario, 6916, 676881, 1.0.25472, , ame,

PUM.Optional.DisableMRT,

HKLM\SOFTWARE\WOW6432NODE\POLICIES\MICROSOFT\MRT\DONTOFFERTHROUGHWUAU, Sin acciones por parte del usuario, 6916, 676880, 1.0.25472, , ame,

PUM.Optional.DisableMRT,

HKLM\SOFTWARE\WOW6432NODE\POLICIES\MICROSOFT\MRT\DONTREPORTINFECTIONINFORMATION, Sin acciones por parte del usuario, 6916, 676881, 1.0.25472, , ame,

Datos del registro: 0

(No hay elementos maliciosos detectados)

Secuencia de datos: 0
(No hay elementos maliciosos detectados)

Carpeta: 0
(No hay elementos maliciosos detectados)

Archivo: 0
(No hay elementos maliciosos detectados)

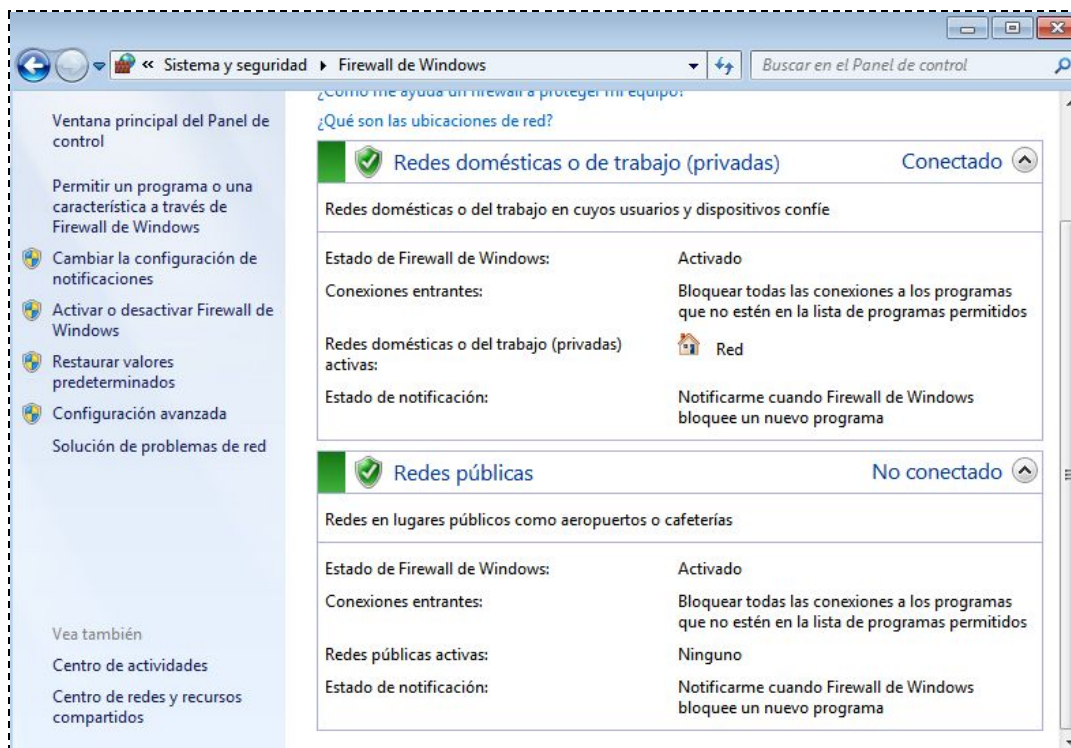
Sector físico: 0
(No hay elementos maliciosos detectados)

WMI: 0
(No hay elementos maliciosos detectados)

(end)

6. Comprueba si tienes un firewall en tu sistema. Si es así, indica cual es y pon una captura. Sino, indícalo y busca un posible candidato (indicando por qué lo elegirías). No hace falta que lo instales.

Windows 7 ya posee un firewall integrado:



7. Abre un navegador y visita la página:

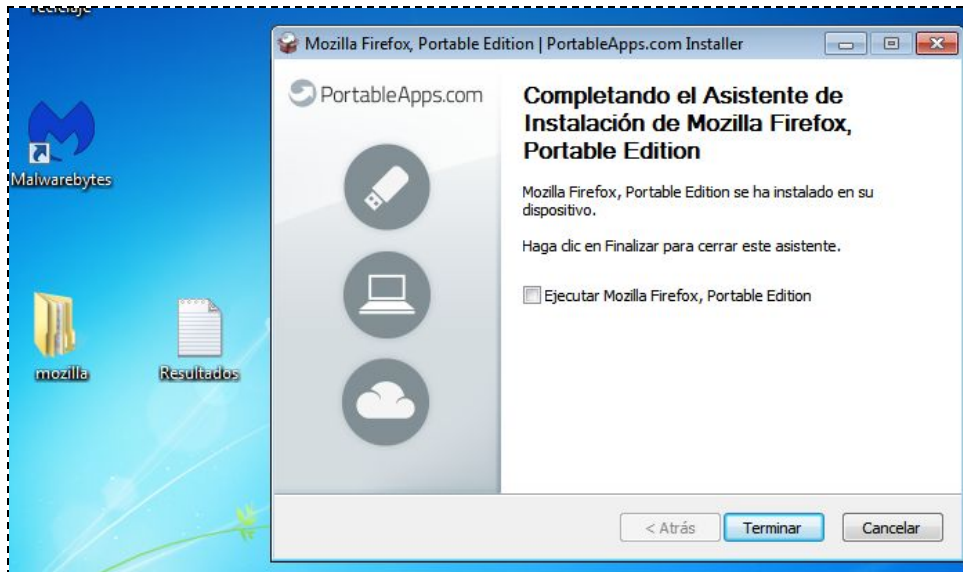
https://portableapps.com/apps/internet/firefox_portable

8. Descarga esa versión del navegador y ejecútala (Si tienes Firefox instalado en el equipo, no te preocupes, no va a afectar en nada a la versión que tengas ya instalada). ¿Puedes

ejecutarla correctamente (te pide clave o algo)? ¿Por qué ocurre eso?

No solicita ninguna contraseña, se “instala” correctamente:

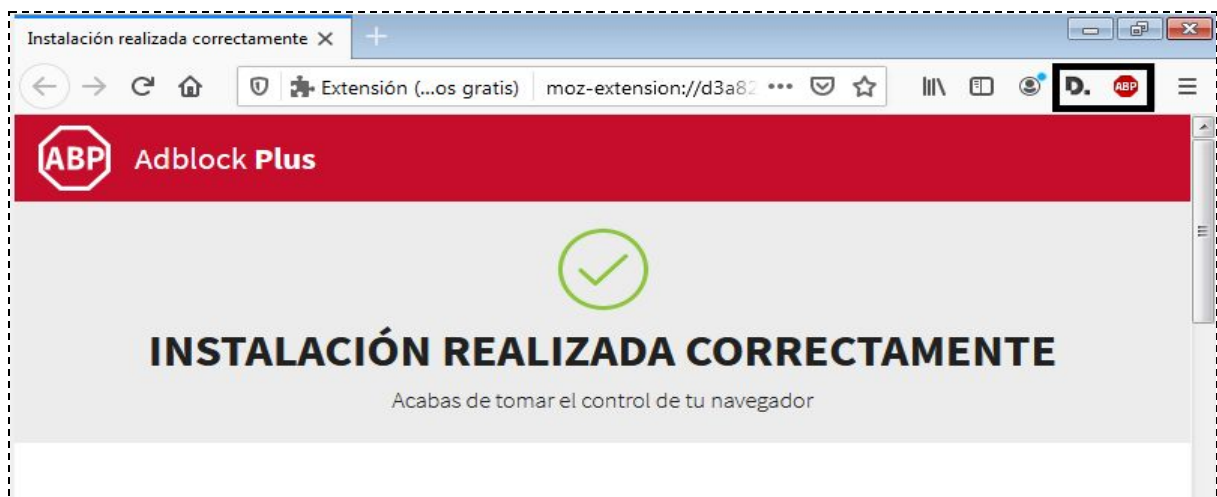
-



Esto ocurre porque se trata de una versión portable. Estas versiones no necesitan ser instaladas. Se trata de un archivo comprimido cuya instalación descomprime los ficheros necesarios para ejecutar la aplicación. La diferencia con la versión base de Firefox es que una vez cierras la aplicación no deja ningún rastro en el ordenador.

9. Instala el complemento ADBLOCK PLUS (o similar) y el complemento DISCONNECT en el navegador que has descargado. ¿Son útiles esos complementos? ¿Por qué?

Una vez instalados ambos addons en Firefox, aparecen como iconos de acceso directo en la barra superior del navegador:



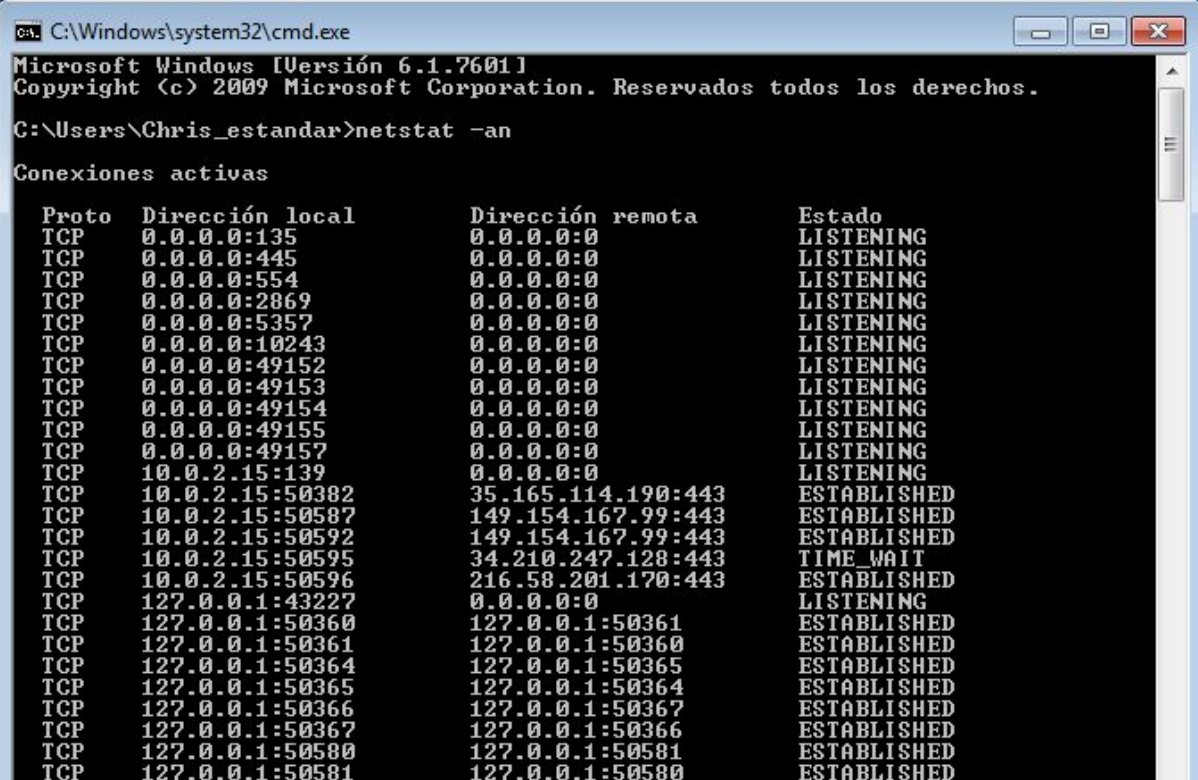
Adblock Plus permite bloquear anuncios intrusivos a la hora de acceder a las páginas webs

reduciendo el riesgo de infección además de permitir navegar más rápido. Por otro lado, Disconnect es un complemento que bloquea las herramientas de tracking que se activan sin nuestro permiso.

Son, entre otros, complementos secundarios que aseguran una navegación más segura y rápida.

10. Abre una consola de comandos en tu sistema operativo y escribe: netstat -an. ¿Qué significa esa información?

La ejecución del comando netstat permite conocer información sobre las conexiones que establece el equipo. Con 'a', muestra todas las conexiones y puertos a la escucha y con 'n' muestra las direcciones y puertos en formato numérico.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\Chris_estandar>netstat -an

Conexiones activas

Proto  Dirección local      Dirección remota      Estado
TCP    0.0.0.0:135           0.0.0.0:0             LISTENING
TCP    0.0.0.0:445           0.0.0.0:0             LISTENING
TCP    0.0.0.0:554           0.0.0.0:0             LISTENING
TCP    0.0.0.0:2869          0.0.0.0:0             LISTENING
TCP    0.0.0.0:5357          0.0.0.0:0             LISTENING
TCP    0.0.0.0:10243         0.0.0.0:0             LISTENING
TCP    0.0.0.0:49152         0.0.0.0:0             LISTENING
TCP    0.0.0.0:49153         0.0.0.0:0             LISTENING
TCP    0.0.0.0:49154         0.0.0.0:0             LISTENING
TCP    0.0.0.0:49155         0.0.0.0:0             LISTENING
TCP    0.0.0.0:49157         0.0.0.0:0             LISTENING
TCP    10.0.2.15:139         0.0.0.0:0             LISTENING
TCP    10.0.2.15:50382       35.165.114.190:443    ESTABLISHED
TCP    10.0.2.15:50587       149.154.167.99:443    ESTABLISHED
TCP    10.0.2.15:50592       149.154.167.99:443    ESTABLISHED
TCP    10.0.2.15:50595       34.210.247.128:443    TIME_WAIT
TCP    10.0.2.15:50596       216.58.201.170:443    ESTABLISHED
TCP    127.0.0.1:43227       0.0.0.0:0             LISTENING
TCP    127.0.0.1:50360       127.0.0.1:50361       ESTABLISHED
TCP    127.0.0.1:50361       127.0.0.1:50360       ESTABLISHED
TCP    127.0.0.1:50364       127.0.0.1:50365       ESTABLISHED
TCP    127.0.0.1:50365       127.0.0.1:50364       ESTABLISHED
TCP    127.0.0.1:50366       127.0.0.1:50367       ESTABLISHED
TCP    127.0.0.1:50367       127.0.0.1:50366       ESTABLISHED
TCP    127.0.0.1:50580       127.0.0.1:50581       ESTABLISHED
TCP    127.0.0.1:50581       127.0.0.1:50580       ESTABLISHED
```