Seguridad en la Red

Transcribed on August 4, 2025 at 10:31 AM by Minutes AI

Speaker 1 (00:04)

Bienvenidos a esta nueva sesión de la seguridad en la parte de red.

Hablaremos de los diferentes elementos que vamos a tener en la configuración para poder conectarnos a la red, qué importancia tienen esas configuraciones en la parte de seguridad y luego hablaremos del firewall de Windows, que es otro elemento que tiene una vital importancia en lo que se refiere a la seguridad de las conexiones de red.

El primer paso para poder entender la seguridad de un dispositivo es verificar la configuración del adaptador o los adaptadores de red.

De esta manera vamos a asegurarnos que no haya una configuración inadecuada, que no haya una configuración extraña y tenemos que verificar todas las partes específicamente de la configuración de los adaptadores de red.

El siguiente paso es verificar aquellos elementos que están compartidos y después cómo está configurado el dispositivo en lo que se refiere a la parte de recursos compartidos.

Los recursos compartidos que nosotros tenemos en una red privada, es decir, cuando nosotros queremos acceder a una impresora, cuando nosotros queremos acceder a una carpeta compartida, cuando un servidor o un determinado elemento de nuestra infraestructura necesita conectarse con mi equipo para hacer algún tipo de operación, pues vamos a tener que tener una serie de servicios, una serie de elementos que van a permitir esas conexiones.

Esos mismos elementos que tenemos abiertos, esas mismas configuraciones que tenemos que permiten esas conexiones fuera del entorno de nuestra red empresarial o del entorno de nuestra red local, pueden ser un peligro de seguridad.

Entonces hay que tener en cuenta qué estamos compartiendo, qué características del sistema operativo tenemos habilitadas para buscar recursos compartidos dentro de la red y si esos elementos tienen que estar configurados o tienen que aprobar esas conexiones en función de donde esté el dispositivo.

Esto tiene especial importancia cuando hablamos de dispositivos portátiles.

Cuando yo tengo un ordenador portátil, una tablet o un móvil, ese dispositivo se va a mover geográficamente y habrá momentos en los que yo esté en una red de confianza dentro de mi organización o esté en una red de confianza dentro de mi hogar, pero va a haber otros momentos en los que ese dispositivo va a estar conectado a una red pública, bien porque estoy en un hotel, o porque estoy en un restaurante o porque estoy viajando.

Y esto lo que va a hacer es que si yo tengo abiertos esos servicios para buscar recursos compartidos se puede generar un riesgo de seguridad importante dentro de los sistemas operativos Windows.

También podemos personalizar cómo va a funcionar el navegador basándonos en una serie de zonas de seguridad que van a ser Internet, la red local interna, sitios de confianza o sitios restringidos.

Cada una de estas zonas se puede configurar con un nivel de seguridad diferente y esto va a determinar el tipo de contenido que va a bloquear.

No sólo el tipo de contenido, va a decidir también si se puede ejecutar JavaScript, si se pueden ejecutar complementos, si se pueden descargar ciertos elementos, si pueden funcionar cierto tipo de software o cierto tipo de aplicaciones.

Y puede marcar la diferencia entre que una web maliciosa sea capaz de hacer un ataque sobre el dispositivo o pueda ejecutar algo en la parte del dispositivo o que no pueda hacerlo.

Por último, otro elemento que debemos tener siempre controlado en lo que se refiere a la parte de seguridad de red son los servicios.

Esto es especialmente importante en los servidores, pero también tenemos que controlarlo en los equipos cliente.

Entonces nosotros vamos a poder ver los servicios que están funcionando, que están a la escucha tanto con el comando sc list o a través de la consola de servicios.

Incluso la consola de servicios podemos conectar desde el administrador de tareas y podemos tener una vista previa desde el propio administrador de tareas para ver qué servicios se están ejecutando en nuestro dispositivo.

Una vez que estamos en la máquina virtual nos vamos a Inicio, nos vamos a Configuración, nos vamos a la parte de configuración de red y tenemos aquí la configuración de Ethernet.

Podemos seleccionar si queremos estar conectados a una red pública o una red privada.

También tenemos la posibilidad de hacer una configuración de autenticación para el protocolo IEX y después tendríamos la posibilidad de editar aquí diferentes valores, como puede ser si queremos que la IP se asigne a través de DHCP, el servicio de DNS o copiar información sobre la configuración del adaptador de red.

Otras opciones que tenemos disponibles sería la configuración de una VPN, el modo avión, la configuración del proxy y luego tendríamos la configuración avanzada de la parte de red.

En la parte de configuración avanzada nosotros vamos a tener aquí la configuración de Ethernet y dentro de la parte de configuración de Ethernet podemos renombrar el adaptador o podemos aquí editar directamente las propiedades del adaptador de red.

Desde aquí nosotros podemos ver cómo está configurado por ejemplo el protocolo TCP IPV, podemos ir a la parte de propiedades, podemos ir a la parte de avanzado y podemos ver cómo está configurado.

Podemos ver cómo está configurado la parte de DNS o cómo está configurada la parte de WINS.

Lo mismo podríamos hacer también con el protocolo de TCP IPV, podríamos ir a la parte de propiedades y ver la configuración que tenemos asociada al protocolo.

Y en la parte de avanzado tendríamos aquí la configuración y tendríamos aquí el servicio de DNS.

Aparte de revisar las opciones del adaptador, nosotros tenemos también aquí la posibilidad de trabajar con las opciones de recursos compartidos.

Entonces en función del perfil con el que nosotros estemos trabajando, por ejemplo en este caso sería una red pública, pues las opciones de compartir archivos o impresoras o el descubrimiento de red estaría deshabilitado.

En la parte de redes privadas sí que tendríamos habilitado el descubrimiento de red, aunque los servicios de compartir archivos e impresoras estarían desactivados hasta que nosotros los activemos porque tengamos la necesidad de que estén activos para una determinada función.

También podríamos ver las propiedades de hardware y luego desde aquí tendríamos también las opciones de Internet.

Desde aquí nosotros en las propiedades de Internet podemos ir a la parte de seguridad y vamos a ver la zona de Internet, la zona local de intranet, las zonas de confianza y los sitios restringidos.

Cada uno de estos elementos nosotros podemos personalizarlo, podemos revisar y configurar de forma manual cada uno de los complementos que vamos a permitir que estén habilitados cuando el navegador detecta que está en una zona de confianza o que está en una zona de Internet y vamos a decidir si permitimos descarga, si se puede ejecutar puntos, se pueden ejecutar diferentes complementos o diferentes servicios relacionados con lo que sería la parte de seguridad de las conexiones del navegador.

Otro elemento que debemos tener en cuenta es la revisión de los servicios.

Para ello si nosotros vamos al administrador de tareas, en la parte del administrador de tareas vamos a tener aquí la parte de servicios.

Entonces nosotros podemos ver aquí los diferentes servicios, podemos ver si esos servicios están detenidos o esos servicios están iniciados o el grupo al que pertenecen esos determinados servicios.

Desde aquí nosotros podemos abrir la consola de servicios que tiene mucha más información y una vez que abrimos la consola de servicios no solo vamos a ver los servicios que tenemos ejecutándose, tendríamos también una descripción de dichos servicios, el modo en el que están, el status si están ejecutándose y después tendríamos también dos elementos que son uno, el modo de inicio de ese servicio, si se arranca de forma automática, se arranca de forma manual, de forma manual retardada y después la cuenta que se utiliza para trabajar con ese servicio.

Esto tiene especial importancia porque como hemos visto anteriormente, no todas las cuentas tienen los mismos privilegios, entonces no es lo mismo local system que network service, que localService, entonces en función de que se esté ejecutando una determinada cuenta, pues va a tener una serie de privilegios o va a tener otra serie de privilegios diferentes.

Otro elemento fundamental en lo que se refiere a la parte de la administración de seguridad es el Firewall de Windows.

Es importante entender que el Firewall de Windows va a trabajar sobre tres perfiles diferentes de conexión que son los que hemos visto en la parte del adaptador de red.

Tiene un perfil de dominio, tiene un perfil privado y tiene un perfil público.

¿Qué quiere decir esto?

Que cuando nosotros nos conectamos a una red vamos a definir una determinada conexión, un determinado perfil.

Entonces si nosotros estamos dentro de la red local, nosotros vamos a necesitar conectarnos a la impresora, conectarnos a una carpeta compartida y el Firewall de Windows va a abrir esos puertos y va a permitir esas conexiones.

Cuando nosotros estamos en una red pública, que no es una red de confianza, todos esos puertos deben mantenerse cerrados.

Cuando nosotros estamos configurando el Firewall de Windows tenemos que entender que trabaja en estos tres perfiles y cuando generamos una regla tenemos que entender que esa regla del firewall en qué perfil se debe de aplicar.

Si yo voy a abrir una regla para permitir una conexión, una solicitud de eco, es decir, que me puedan hacer PIN al dispositivo para revisar la conexión de ese dispositivo, pues esa regla la voy a poner en el perfil privado o la voy a poner en el perfil de dominio, pero nunca la voy a poner en el perfil público, porque yo entiendo que cuando mi dispositivo está en un hotel o está en un restaurante o está en un aeropuerto, nadie va a tener la necesidad de realizar una comprobación de conexión, nadie debería hacer ping a mi dispositivo, nadie debería tratar de localizar carpetas compartidas en mi dispositivo.

Cuando yo estoy en una red externa.

Entonces esto debemos tenerlo en cuenta cuando estamos configurando el Firewall de Windows.

Luego las reglas de entrada o de salida del Firewall nos van a permitir definir qué conexiones entrantes o qué conexiones salientes vamos a tener disponibles en el equipo.

Además podemos exportar esas reglas.

También tenemos la posibilidad de habilitar las notificaciones cuando el firewall bloquea una nueva aplicación.

Entonces cuando nosotros tenemos una aplicación que no funciona o que no se puede conectar al dispositivo porque está deteniéndola el firewall, nos va a aparecer un mensaje y desde ese mismo mensaje nosotros podemos habilitar una regla de permitir una excepción para esa determinada aplicación.

Luego tenemos las reglas de seguridad de la conexión, es una de las partes más interesantes del Firewall de Windows.

Las reglas de seguridad de la conexión nos van a permitir definir cómo se conectan uno o varios dispositivos, un dispositivo con muchos o muchos con uno o muchos con muchos o uno con uno.

Y además nos va a permitir definir cómo van a ser las reglas de esas conexiones, Si hay autenticación en uno de los extremos, si hay autenticación en los dos extremos, si la comunicación tiene que estar cifrada.

Y esto nos va a dar una capa adicional de seguridad dentro de la propia red interna, porque yo puedo hacer que cuando una serie de dispositivos se conectan con unos determinados servidores estén protegidos a través de IPSec, haya autenticación en los dos extremos y además ese tráfico esté cifrado.

Si hay un atacante que está realizando un análisis de la red o está capturando el tráfico de la red desde la parte interna de la organización, pues no va a poder capturar ese tráfico o le vamos a dificultar que pueda acceder a ese tráfico.

Dentro de las reglas de conexión podemos habilitar las reglas de túnel que va a funcionar con IPSec y que va a utilizar cifrados con protocolos como DES, 3, DES o AES.

Puede ser una capa adicional de seguridad en ciertos entornos.

Desde la propia configuración avanzada de red vamos a tener un enlace para acceder al Firewall de Windows.

Una vez que accedemos al Firewall de Windows, aquí vamos a ver cada uno de los perfiles.

En este caso vemos que este equipo está conectado a una red pública y es el perfil que tiene habilitado por defecto.

Podemos habilitar que una aplicación pase a través del Firewall de Windows, podríamos hacerlo desde aquí, Podríamos tener ejecutar el solucionador de errores de acceso a Internet si tenemos algún problema de comunicación.

Y si nos vamos a la parte de configuración avanzada, en la parte de configuración avanzada es donde nosotros vamos a tener la posibilidad de configurar las reglas de entrada.

Aquí si quisiéramos crear una regla diríamos nueva regla.

También podemos crear reglas de salida, daríamos aquí a nueva regla y crearíamos una regla de salida y tendríamos aquí la posibilidad también de monitorizar el tráfico del firewall.

Si nos vamos a las reglas de seguridad de la conexión, creamos una nueva regla, vamos a una regla personalizada, damos a siguiente y aquí seleccionamos el origen y el destino de los elementos que queremos comunicar.

Seleccionamos por ejemplo desde unas determinadas IPs y podemos seleccionar una determinada IP, Podemos seleccionar un rango de red, en este caso vamos a seleccionar un rango de red, toda la red 13.0.

Podemos seleccionar el destino, por ejemplo, podemos seleccionar el destino a un determinado servidor o a un determinado grupo de servidores o a un determinado rango, desde una dirección determinada a una dirección determinada.

Imaginaros que lo que queremos hacer es a un determinado servidor, es decir, a una IP específica.

Aquí podemos solicitar la autenticación de entrada o de salida para las conexiones o podemos requerir la autenticación de entrada o de salida para las conexiones.

Si nosotros vamos a hacer una solicitud no va a detener la comunicación, pero sí que va a tratar de solicitar ese proceso de autenticación.

Si nosotros vamos a requerir, automáticamente va a obligar a ese servicio a que haya ese proceso de autenticación o si no va a cortar la comunicación.

Podemos seleccionar diferentes mecanismos para este proceso de autenticación, puede ser a través de IPSec, puede ser a través de Kerberos o podemos seleccionar nosotros y personalizar como queremos que sea el servicio de autenticación.

Podemos añadir aquí y vemos que nos aparece nuevamente Kerberos NTLM, servicios de certificados, donde especificaríamos la autoridad certificadora o incluso una clave compartida.

Una vez que nosotros tenemos ese determinado servicio, podemos añadir si queremos más factores de autenticación para que haya más de un factor de autenticación daríamos a OK, daríamos a siguiente y aquí seleccionamos también si queremos el determinado protocolo que nosotros queramos, por ejemplo podemos seleccionar TCP y TCP, podemos seleccionar una serie de puertos específicos y podemos seleccionar el puerto 80 y el puerto 445.

Daríamos a siguiente, seleccionamos el perfil, en este caso estoy creando una regla, por ejemplo para una conexión privada o una conexión de dominio.

Seleccionamos un nombre para la regla y daríamos a finalizar.

Para concluir es esencial verificar las conexiones, empezando por revisar las configuraciones del propio adaptador de red, las propias configuraciones de compartición y de búsqueda de recursos compartidos.

Es importante entender cómo funciona el firewall de Windows, que puede ser un excelente aliado para aumentar la seguridad de las conexiones de red y la seguridad de una organización dentro de la propia red interna.

También es necesario controlar la ejecución de servicios, deshabilitar aquellos servicios que no necesitamos o verificar que no se pueda acceder a esos servicios cuando estamos en una red que no es de confianza.

Hay una propuesta de ejercicio para este tema, que es configurar una regla de tráfico entrante en el Fargo que sólo permita solicitudes de PIN.

Esto lo vamos a hacer a través de la configuración de reglas de entrada en la seguridad avanzada del firewall.

En el siguiente vídeo corregiremos ese ejercicio.

Llegamos al final de la sesión.

Os esperamos en el siguiente vídeo.