Introducción

Independientemente del software que esté ejecutando, existen dos problemas de seguridad importantes cuando se alojan sitios Web desde el equipo.

Proteger el equipo frente a usuarios no autorizados. El alojamiento de sitios Web, incluso en una intranet, abre el equipo host a una comunidad más amplia de usuarios. La autenticación es el proceso que consiste en permitir a los usuarios el acceso a un servicio Web, basándose en nombres de usuario y contraseñas o en direcciones IP. (La restricción de usuarios mediante direcciones IP es menos segura, ya que los usuarios más hábiles pueden "imitar" una dirección IP y conseguir acceso al (equipo host.)

Proteger el equipo frente a programas malintencionados. El contenido de un sitio Web puede hacer que los programas se ejecuten en el equipo host. Una página HTML que "incluye" o "sustituye" a otra página puede hacer que un programa se ejecute en el equipo host. Al marcar los directorios como ejecutables, de modo que se pueda ejecutar una secuencia de comandos en el equipo host, un programa puede realizar cualquier operación dentro de los límites impuestos por el esquema de protección de recursos del equipo host.

Las páginas HTML pueden contener controles incrustados, secuencias de comandos, subprogramas y otros programas que pueden hacer que se ejecuten programas en un equipo host. Los controladores de formularios pueden suponer un riesgo adicional, ya que existe la posibilidad de que los usuarios emitan comandos desde campos de los formularios, lo que hará que se ejecuten los programas cuando se explore la página que contiene los resultados del formulario. (Los controladores de formularios de Microsoft® FrontPage® no lo permiten.)

FrontPage soluciona estos problemas de seguridad mediante los mecanismos de seguridad integrados del equipo host. El uso de las Extensiones de servidor de FrontPage no requiere realizar cambios en el método de seguridad del equipo host.

En los servidores Web de Servicios de Internet Information Server (IIS) basados en Microsoft® Windows NT®, cada petición HTTP a IIS desde un explorador de Web o el cliente de FrontPage se ejecuta bajo una cuenta de usuario del sistema operativo Windows NT que aloja IIS. FrontPage implementa la seguridad Web en IIS mediante la modificación de las listas de control de acceso, correspondientes a todos los archivos y carpetas de cada Web extendido con FrontPage.

En los servidores Web basados en UNIX, el servidor mantiene una lista de cuentas con nombres de usuario y contraseñas y una lista de grupos de usuarios, todos con distintos niveles de permisos para el uso de servicios del servidor Web. Las cuentas y los grupos que mantiene el servidor Web son independientes de la lista de usuarios y grupos con acceso al sistema de archivos del equipo host. Al crear los archivos de acceso a través del contenido del servidor Web, diferentes grupos de usuarios, con distintos niveles de permiso, pueden tener acceso a diferentes áreas del servidor.

FrontPage cuenta con este mecanismo para agregar a la lista de cuentas del servidor Web administradores de Web, autores y visitantes del sitio con los permisos adecuados, y proteger el contenido y los programas de los sitios Web extendidos con FrontPage.

Modelo de seguridad de Windows NT

En Microsoft® Windows NT®, un administrador o un programa pueden conceder a los usuarios y grupos varios niveles de acceso a los recursos del sistema. Los usuarios con cuentas en Windows NT deberán presentar sus credenciales de identificación (nombre de usuario y contraseña) antes de poder tener acceso a un

recurso de Windows NT. Las cuentas de grupo también se encuentran disponibles en Windows NT.

Éstas no tienen contraseñas, pero son una manera útil de conceder privilegios a varias cuentas de usuario a la vez. Windows NT ejecuta aplicaciones especiales denominadas servicios. Los servicios son programas que se inician junto con el sistema operativo y se ejecutan en un segundo plano, sin ninguna interfaz de usuario. (El servidor Web IIS es un servicio.) Los servicios, junto con todas las aplicaciones que se ejecutan en Windows NT, deben ejecutarse en el contexto de una cuenta de usuario, representada por un testigo.

Testigos e identificadores de seguridad

Un testigo identifica a un usuario y a los grupos de Windows NT a los que pertenezca dicho usuario. También contiene el identificador de seguridad del usuario (SID) y los SID de todos los grupos a los que pertenece el usuario. Un SID solamente identifica a cada usuario y grupo de Windows NT. Los programas de Windows NT se ejecutan en el contexto de un testigo. Cuando un programa inicia otro programa, pasa su testigo al nuevo programa.

Listas de control de acceso

Una lista de control de acceso (ACL) es una lista de entradas asociadas a un archivo o carpeta que especifica qué usuarios y grupos tienen acceso a esa carpeta o archivo. Cada entrada de una ACL asigna a un usuario o grupo uno o varios de los siguientes niveles de acceso a archivos:

Ninguno no permite al usuario tener acceso a ningún archivo.

Lectura (Lectura de datos en Windows 2000) permite que un usuario vea los datos de un archivo.

Escritura (Escritura de datos en Windows 2000) permite al usuario modificar los datos de un archivo.

Ejecución (Ejecución de archivo en Windows 2000) permite que un usuario ejecute el archivo de un programa.

Eliminación permite a un usuario eliminar un archivo.

cambio de permisos permite a un usuario cambiar los permisos de un archivo.

Toma de posesión permite a un usuario tomar posesión de un archivo.

Se establece un conjunto de privilegios similares en las carpetas:

Ninguno no permite al usuario tener acceso a las carpetas.

Lectura (Enumerar carpetas en Windows 2000) permite a un usuario ver nombres de archivo y de subcarpetas.

Escritura (Crear archivos en Windows 2000) permite al usuario agregar archivos y subcarpetas.

Ejecución (Cambiar nivel de carpeta en Windows 2000) permite al usuario cambiar a subcarpetas.

Eliminación (Eliminar subcarpetas y archivos en Windows 2000) permite a un usuario eliminar una subcarpeta.

Cambio de permisos permite a un usuario cambiar permisos en una carpeta.

Toma de posesión permite a los usuarios tomar posesión de una carpeta.

Windows NT Y Windows 2000 admiten dos tipos de particiones de archivo: NTFS y FAT. Únicamente NTFS admite ACL. Puesto que la seguridad de las extensiones de servidor de Microsoft® FrontPage® se basa en las ACL, deberá utilizar NTFS en un sistema en el que aloje servicios del World Wide Web mediante IIS y FrontPage.

Representación del usuario

Cuando se ejecuta una aplicación, ésta "representa" al usuario que se haya autenticado para utilizar la aplicación. A continuación, cuando la aplicación intente llamar a otra aplicación o utilice un recurso del sistema como el sistema de archivos, el acceso a la nueva aplicación o a recursos del sistema se obtiene o no en función de los permisos del usuario representado. Al hacer que las aplicaciones se ejecuten como usuario, Windows NT garantiza que dichas aplicaciones únicamente tendrán acceso a los recursos del sistema a los que pueda tener acceso el usuario que está ejecutando esas aplicaciones. Además, la representación reduce el número de veces que es necesario que el usuario escriba una contraseña, ya que puede invocarse una gran variedad de aplicaciones y servicios del sistema una vez haya autentificado el usuario.

La representación también funciona de forma remota. Si un usuario dispone de los privilegios adecuados en un equipo remoto, una aplicación que se encuentra en dicho equipo representará al usuario que la haya llamado de manera remota. Por ejemplo, cuando un usuario con privilegios de edición sobre un servidor remoto de Windows NT intente crear contenido en un servidor, la DLL de edición de FrontPage se ejecutará como el usuario representado, lo que garantizará que el usuario únicamente tendrá acceso a archivos que se encuentren disponibles para esa cuenta de usuario.

Métodos de autenticación de IIS

Todos los usuarios deben estar autenticados antes de obtener acceso a los recursos de IIS. IIS admite autenticación anónima, autenticación básica, autenticación Desafío/Respuesta de Windows NT y autenticación de acceso implícita.

Autenticación anónima

La autenticación anónima proporciona acceso, mediante una cuenta especial "anónima", a usuarios que no disponen de sus propias cuentas en el equipo host. Cada servicio Internet, como el servicio World Wide Web o el servicio FTP, utiliza una cuenta de Windows NT (un nombre de usuario y una contraseña) para procesar peticiones anóminas. Internet Information Server (IIS) crea la cuenta anónima para servicios web, USR_nombre de equipo, durante su instalación. De manera predeterminada, todas las peticiones del cliente Web usan esta cuenta y los clientes tienen acceso al contenido Web cuando la utilizan. Podrá habilitar al mismo tiempo el acceso de inicio de sesión anónimo y el acceso autenticado.

Cuando IIS recibe una petición anónima, representa la cuenta de inicio de sesión anónima. La petición tendrá éxito si la cuenta anónima dispone de permiso para tener acceso al recurso solicitado; el que la cuenta tenga permiso o no, se determina mediante la ACL de recursos. Si la cuenta anónima no tiene permiso, la petición no tendrá éxito. El servicio WWW responde a una petición anónima fallida solicitando al usuario que suministre un nombre de usuario y una contraseña de Windows NT válidos.

Autenticación básica

La autenticación básica es un método de autenticación admitido por la mayoría de los servidores Web de Internet. Cuando un servidor utiliza una autenticación básica, el explorador de Web (o el cliente FrontPage) pedirá al usuario un nombre y una contraseña. A continuación, el nombre de usuario y la contraseña se

transmiten por HTTP, en texto simple. Mediante este nombre de usuario y esta contraseña, IIS autentica al usuario de Windows NT correspondiente.

En la autenticación básica, el usuario siempre inicia la sesión con derechos locales de inicio de sesión, lo que es similar al inicio de sesión del usuario para una sesión interactiva en la consola del equipo. (Para utilizar la autenticación básica, conceda a cada cuenta de usuario el derecho de usuario a Inicio de sesión local en el servidor IIS.) Existen dos posibles problemas causados por el usuario del inicio de sesión local de la autenticación básica que los administradores deberían tener en cuenta:

La autenticación básica no tendrá éxito si la cuenta de usuario no dispone de derechos de inicio de sesión local. Incluso aunque parezca que la configuración de FrontPage, IIS y Windows NT es correcta, la falta de derechos de inicio de sesión local, concedidos al usuario en el Administrador de usuarios de Windows NT, evitará que la autenticación básica autentique al usuario. Con el inicio de sesión local, si un usuario puede obtener acceso físico al equipo host que ejecuta IIS, tendrá permiso para iniciar una sesión interactiva en la consola.

Otro riesgo de seguridad de la autenticación básica es que los nombres de usuario y las contraseñas se transmiten por la red en un formato que puede descodificarse fácilmente.

Si el sitio Web debe ser compatible con la autorización del cliente FrontPage versión 1.1 (que no es compatible con la autenticación Desafío/Respuesta de Windows NT) o si desea asegurarse de que se puede tener acceso al sitio Web desde todos los tipos de exploradores, deberá tener habilitada la autenticación básica. Además, la autenticación básica funciona por un servidor de seguridad mediante un servidor proxy. Si los usuarios establecen una conexión con el servidor Web de Internet mediante un servidor proxy, deberá utilizar la autenticación básica en vez de la de Desafío/Respuesta de Windows NT.

La autenticación básica es más rápida que la de Desafío/Respuesta de Windows NT. Si utiliza la autenticación básica junto con Secure Sockets Layer (SSL), podrá disponer de una autenticación segura y rápida.

Autenticación Desafío/Respuesta **de** Windows NT

La autenticación Desafío/Respuesta de Windows NT (también denominada NTLM) es un método de autenticación más seguro que el de autenticación básica. Cuando se autentica un usuario mediante Desafío/Respuesta de Windows NT, inicia una sesión en el equipo del servidor Web como un inicio de sesión en la red. En primer lugar, el explorador de Web o el cliente FrontPage intentan utilizar las credenciales que el usuario suministró al iniciar la sesión en el equipo cliente.

Si dichas credenciales se rechazan, la autenticación de desafío/Respuesta de Windows NT pedirá al usuario un nombre y una contraseña mediante un cuadro de diálogo. Si un usuario ha iniciado la sesión como usuario de dominio en un equipo local, dicho usuario no tendrá que autenticarse de nuevo cuando tenga acceso al equipo remoto de ese dominio.

El nombre de usuario y la contraseña se codifican de manera segura en una interacción de varias transacciones entre el cliente y el servidor Web. Esta interacción es segura frente a los espías de la red que intenten entrar en los sistemas mediante el control del tráfico de la red entre un cliente y un servidor.

Existen ciertas limitaciones del Desafío/Respuesta de Windows NT:

La autenticación Desafío/Respuesta de Windows NT no puede llevarse a cabo con un servidor de seguridad mediante un servidor proxy. En este escenario, los usuarios deben utilizar la autenticación básica. Algunos exploradores de Web (por ejemplo, Netscape Navigator) no admiten la autenticación Desafío/Respuesta de Windows NT.

La autenticación Desafío/Respuesta de Windows NT no admite la delegación en servidores secundarios. Las credenciales del usuario no pueden pasar a otro equipo. Por ejemplo, cuando una petición llega a IIS, las credenciales de la cuenta de usuario no pueden pasar a Microsoft SQL Server en un equipo secundario.

Puesto que la autenticación Desafío/Respuesta de Windows NT no puede llevarse a cabo mediante un servidor de seguridad, es más útil en las intranet, donde la comunicación tiene lugar dentro del servidor de seguridad de la organización.

Es posible habilitar tanto la autenticación básica como la autenticación Desafío/Respuesta de Windows NT. Si el explorador de Web admite la autenticación Desafío/Respuesta de Windows NT, utilizará ese método de autenticación. Si no, utilizará la autenticación básica. En la actualidad, únicamente Microsoft Internet Explorer 2.0 o versiones posteriores admiten la autenticación Desafío/Respuesta de Windows NT.

Autenticación de acceso implícita

De igual manera que la autenticación básica, la autenticación de acceso implícita se basa en un sencillo método de Desafío/Respuesta. Lanza un desafío mediante un valor de una sola vez (una cadena de datos especificados por el servidor que únicamente pueden generarse cada vez que se comete un error 401). Una respuesta válida contiene una suma de comprobación del nombre de usuario, la contraseña, el valor de una sola vez dado, el método HTTP y la dirección URL solicitada. De esta forma, la contraseña nunca se envía como texto que pueda descodificarse fácilmente, que es el punto débil más importante de la autenticación básica.

La autenticación de acceso implícita requiere Internet Explorer 5.0 en el equipo cliente.

Cómo autentica IIS las peticiones HTTP

Cuando IIS recibe una petición HTTP de un explorador de Web o del cliente FrontPage, lleva a cabo las siguientes operaciones:

1.En primer lugar, la petición se prueba como cuenta anónima, IUSR_nombreDeEquipo. Si esa cuenta no tiene acceso suficiente para completar la petición o si IIS no tiene habilitada la exploración anónima, IIS mostrará el mensaje de error 401 ("Acceso denegado").

2.A continuación, IIS lleva a cabo la autenticación del usuario a fin de permitir que el usuario remoto se identifique mediante la autenticación básica o la de Desafío/Respuesta de Windows NT. Si el explorador de Web o el cliente FrontPage utilizan la autenticación Desafío/Respuesta de Windows NT, es posible que el usuario no vea ninguna pregunta, ya que el cliente FrontPage o el explorador de Web suministrará el nombre de usuario y la contraseña del usuario que inicia la sesión desde el equipo cliente.

3.IIS permite el acceso a un archivo del servidor Web únicamente si la ACL de la NTFS correspondiente al archivo, concede los permisos adecuados a la cuenta que el servidor Web va a representar.

Configuración de las listas de control de acceso

Las herramientas de administración para las Extensiones de servidor de FrontPage (las herramientas Fpsrvadm y Fpremadm, las Extensiones de servidor MMC Snap−in de FrontPage y los Formularios de administración HTML para las Extensiones de servidor de FrontPage) modifican las ACL para archivos y carpetas cuando el administrador de un Web extendido con FrontPage utiliza dichas herramientas. Además, el cliente FrontPage establece las ACL en el tiempo de edición. Por ejemplo, cuando un autor crea una nueva carpeta o página en un Web extendido con FrontPage, el cliente FrontPage establece las ACL de la nueva página o carpeta.

En la siguiente tabla se enumera el conjunto de ACL correspondiente a un Web extendido con FrontPage. La primera columna identifica el tipo de carpeta o archivo en el que se establecen las ACL. La segunda columna describe la configuración de la ACL en ese archivo o carpeta. La tercera columna corresponde únicamente a las carpetas. Describe la configuración de la ACL para el nuevo contenido creado en esta carpeta por un autor o administrador que esté utilizando el cliente FrontPage.

Establecer permisos mixtos en el contenido

En FrontPage, los permisos sobre el contenido de un Web extendido con FrontPage se aplican a todo el Web extendido con FrontPage. Todos los autores del Web tienen acceso a todas las páginas del Web, y los visitantes del sitio pueden explorar todas las páginas. En muchas ocasiones, es necesario dividir el contenido de un servidor de manera que diferentes grupos de usuarios tengan permisos para administrar, modificar o explorar diferentes áreas del contenido.

Este tema describe los dos mecanismos que permiten establecer permisos variados en el contenido. Un método consiste en dividir el contenido en tantos subwebs de FrontPage como conjuntos de autores, administradores o visitantes del sitio existan. El otro método consiste en establecer permisos más estrictos sobre el contenido en un solo Web extendido con FrontPage, pero requiere que pase por alto las herramientas de configuración de permisos integradas de FrontPage.

Usar subwebs para establecer **permisos mixto.**

Un subweb extendido con FrontPage es un Web extendido con FrontPage completo que funciona como un subdirectorio del Web raíz o de otro subweb. Los subwebs son el mecanismo recomendado para conceder a distintos grupos de administradores, autores y visitantes del sitio permiso para tener acceso a las diferentes áreas de contenido de un servidor virtual.

Mediante los subwebs se consigue automáticamente una mayor granularidad, ya que cada subweb mantiene configuraciones de seguridad independientes. En versiones anteriores de FrontPage, sólo se podían crear subwebs directamente debajo del Web raíz. En FrontPage 2000, es posible crear subwebs en cualquier nivel de la estructura de contenido, incluido un nivel inferior de otro subweb.

Administrar permisos manualmente

Es posible omitir la administración de seguridad integrada de FrontPage y establecer permisos manualmente en el contenido de un Web extendido con FrontPage. Al elegir este método, puede establecer permisos por carpeta o por archivo, lo que le permite un mayor control granular sobre los permisos en el contenido de un Web, pero tendrá que encargarse de administrar las ACL. Se trata de una técnica avanzada que debe realizarse cuidadosamente para evitar que la seguridad del contenido de su servidor se debilite.

Para establecer permisos manualmente en un Web extendido con FrontPage, abra la consola MMC y utilice el comando Propiedades en el Web extendido con FrontPage. En la ficha Extensiones de servidor, desactive la casilla de verificación Administrar permisos manualmente.

Cuando se administran permisos manualmente en un Web extendido con FrontPage, es necesario modificar las ACL de la carpeta del nivel superior del Web. Como mínimo, a los administradores se les debe dar acceso con permiso de lectura, escritura y edición en la carpeta de nivel superior de un Web o subweb extendido con FrontPage.

Por comodidad, el Asistente para la configuración de las Extensiones de servidor de FrontPage creará tres grupos de equipo local vacíos en el momento en que se cree un Web extendido con FrontPage. Estos grupos se denominarán "nombre de Web Admins", "nombre de Web autores" y nombre de Web Exploradores". Es

recomendable utilizar dichos grupos en las ACL y mantenerlos mediante el Administrador de usuarios de Windows NT.

Inicios de sesión de la red y aplicaciones de delegación

En una aplicación de delegación, una parte del trabajo del servidor Web se delega en un proceso de servidor secundario que se ejecuta en un equipo distinto. Por ejemplo, un servidor Web que tiene acceso a un servidor de base de datos que se ejecuta en un equipo host distinto es una aplicación de delegación.

Si el usuario ha iniciado la sesión localmente, como sucede en la autenticación básica, la seguridad de Windows NT permite que un servidor secundario respete dichas credenciales en una aplicación de seguridad. Si el usuario inició la sesión en la red mediante la autenticación Desafío/Respuesta de Windows NT, las credenciales no se respetan. En este caso, la aplicación de delegación sólo puede ejecutarse si el servidor secundario y el servidor Web se están ejecutando en el mismo equipo host.

Utilizar Secure Sockets Layer

Secure Sockets Layer (SSL) es un protocolo que proporciona privacidad en las comunicaciones, autenticación e integridad de los mensajes en una conexión TCP/IP. Gracias a este protocolo, los clientes y servidores pueden comunicarse de un modo que se eviten escuchas a escondidas, manipulaciones o falsificaciones de mensajes.

Para utilizar SSL en IIS, debe solicitar e instalar un certificado de seguridad y habilitar la configuración apropiada en el cuadro de diálogo Comunicaciones seguras. Para obtener más información, consulte la documentación de IIS.

Con las Extensiones de servidor de FrontPage, SSL garantiza una edición segura mediante servidores de seguridad y garantiza la seguridad durante la administración remota de las Extensiones de servidor de FrontPage.

En el cliente FrontPage, se puede especificar que se utilice SSL al abrir o publicar un Web extendido con FrontPage.