Buenas prácticas de seguridad para servidores windows

Consideraciones básicas de seguridad

- **Deshabilita los usuarios de invitado (guest)**

  En algunas versiones de windows los usuarios de invitado vienen por omisión deshabilitadas pero no en todas. Por ello es importante chequear luego de la instalación en que estatus se encuentra. De igual forma a estos usuarios se les debe asignar una contraseña compleja y se puede restringir el número de logons que puede realizar por día como medida extra de seguridad.

- **Limita el número de cuentas en tu servidor**

  Elimina cualquier usuario innecesario: duplicados (por ejemplo invitado y guest), prueba, compartidos, departamento, etc. Utiliza políticas de grupos para asignar los permisos que se van necesitando. Audita tus usuarios regularmente.

  Las cuentas genéricas son conocidas por contraseñas débiles y muchos accesos desde múltiples equipos. Son el primer punto de ataque de un hacker.

- **Limita los accesos de la cuenta de administración**

  El administrador no debe utilizar la cuenta de mayores privilegios para sus actividades diarias que no necesitan accesos especiales. De esta forma puedes colocarle a la cuenta de administración con todos los privilegios una política de accesos más agresiva: contraseña compleja con cambio cada 3 meses mínimo y un correo o registro de cada acceso de la misma al servidor. De ser posible los administradores sólo deben usar la cuenta de administración una vez que están en el servidor con su cuenta personal y utilizar la cuenta de mayores privilegios en el modo “ejecuta como” o “run as if”, esto permite que sepas quien usaba la cuenta en qué momento y por qué.

- **Renombra la cuenta de administración**

  Aunque se discute aún se discute si esta medida es o no efectiva. Es cierto que al menos dificulta el trabajo de hackers principiantes. La idea es que el nombre del usuario no indique sus privilegios.

- **Crea una cuenta “tonta” de administrador**

  Esta es otra estrategia que se utiliza, crear una cuenta llamada administrador y no se le otorgan privilegios y una contraseña compleja de al menos 10 caracteres. Esto puede mantener a algunas personas que están tratando de acceder entretenidos. Monitorea la utilización de la misma.

- **Cuidado con los privilegios por omisión para los grupos de usuarios**

  En el contexto de windows existen grupos como “Everyone” en el que todo el que entra al sistema tiene acceso a los datos de tu red. Por omisión existen carpetas compartidas para los usuarios del sistema operativo y algunas personas que no conocen los riesgos colocan datos en ellas. Por lo tanto, revisa que grupos pueden acceder a qué carpetas y considera si deben o no tener estos accesos.

- **Coloca las paticiones con NTFS**

  Los sistemas FAT y FAT32 no soportan buenos niveles de seguridad y constituyen una puerta trasera ideal para los atacantes.

- **Configura políticas de seguridad en su servidor y su red**

  Microsoft provee kits de herramientas para la configuración de seguridad a su medida. Estos kits proveen plantillas para seleccionar el nivel de seguridad que su organización requiere y se pueden editar aspectos como: perfil de usuarios, permisología de carpetas, tipos de autenticación, etc. Pata mayor información al respecto puede consultar las páginas de technet de microsoft.

- **Apaga servicios innecesarios en el servidor**

  Por omisión algunos servicios vienen configurados y listos para utilizarse, aquellos que no están siendo utilizados constituyen una vulnerabilidad para su equipo. Revise servicios como: IIS, RAS, terminal services. Estos servicios poseen vulnerabilidades conocidas y deben ser configurados cuidadosamente para evitar ataques. También pueden existir servicios ejecutándose silenciosamente por lo que es necesario auditar periódicamente y verifique que los servicios que están abiertos son aquellos que se están utilizando por usted. Algunos servicios a revisar son los siguientes:

Computer Browser	TCP/IP NetBIOS Helper
Microsoft DNS Server	Spooler
Netlogon	Server
NTLM SSP	WINS
RPC Locator	Workstation
RPC Service	Event Log

- **Cierra el acceso a puertos que no se están utilizando**

  Los servidores son el principal objetivo de un atacante. Una de las estrategias más utilizadas a la hora de localizar una víctima es verificar los puertos que la misma tiene abierta. Por ello, verifique el archivo localizado en: %systemroot%\drivers\etc\services. Configure sus puertos vía la consola de

seguridad TCP/IP ubicada en el panel de control sus accesos de red. Una recomendación general es habilitar específicamente tráfico TCP e ICMP, para ello seleccione la opción de UDP y protocolo IP como permitido únicamente y deje los campos en blanco. Puede conseguir en las páginas de microsoft los puertos abiertos por omisión para el sistema operativo que tiene instalado.

- **Habilita la auditoría en su servidor**

  La forma más básica para detectar intrusos en un sistema operativo microsoft es habilitar las auditorías. Esto le brindará alertas en aspectos de seguridad muy importantes como: cambios en las políticas de seguridad, intentos de rompimiento de claves, accesos no autorizados, modificaciones a privilegios de usuarios, etc. Como mínimo considere habilitar las siguientes opciones: Eventos de login de usuario, gestión de cuentas de usuario, acceso a objetos, cambios en políticas, uso de privilegios y eventos del sistema. Es importante que registre tanto los eventos exitosos como los fallidos ya que ambas le indicaran que una persona no autorizada está tratando de realizar actividades en su servidor.

- **Coloca protección a sus archivos de registros de eventos**

  Por omisión los archivos de eventos no están protegidos es importante dar permisos tanto de lectura como escritura solo a los usuarios de sistema y administradores. De lo contrario un atacante podrá fácilmente eliminar sus huellas luego de un ataque.

- **Desactiva la opción del último usuario para desplegarse en la pantalla de inicio o bloqueo del sistema**

  En windows por omisión cuando se presiona Ctrl-Alt-Del aparece el último usuario que utilizó el equipo esto hace muy fácil obtener el nombre de la cuenta de usuario de administración, el atacante puede utilizar sus habilidades para adivinar o crackear la contraseña del usuario. Este parámetro de configuración puede modificarse en las plantillas de su CD de instalación o en las políticas de seguridad.

- **Verifica los parches de seguridad que libera microsoft mensualmente**

  Microsoft libera boletines de seguridad mensualmente indicando parches para sus sistemas operativos, es indispensable estar al tanto de los mismos y aplicar metódicamente para evitar ser víctima de ataques conocidos y ya reparados. Usted puede suscribirse a listas de actualización en las que le indicaran qué parches están disponibles y en dónde descargarlos.

- **Deshabilita las carpetas compartidas por omisión que no son necesarias**

  Colocando net share en la línea de comando del prompt podrás conocer las carpetas

compartidas.

- **Deshabilita la opción de creación del archivo dump**

  Aunque esta opción es muy útil para conocer los por menores de un error en el servidor como las causas de los famosos pantallazos azules. También sirve para proveer al atacante de información sensible como contraseñas de las aplicaciones. Puedes deshabilitar esta opción en: panel de control, sistema, propiedades, avanzadas, recuperación y reinicio. Allí deshabilita la opción “escribir información de fallas” a ninguna. Si necesitas conocer las causas de una falla recurrente en el servidor siempre puedes volver a habilitar la opción y verificar qué está sucendiendo. Si lo haces recuerda eliminar los archivos que se creen después de utilizarlos.

Referencias

José F. Torres. Practicas básicas de de seguridad en Windows. 2da. Escuela Venezolana de Seguridad de Cómputo. Agosto 2006.

Universidad Autónoma de Madrid. Guía básica de seguridad para Windows . http://www.uam.es/servicios/ti/servicios/ss/rec/winnt.html

Microsoft Technet. TechNet: Security Guidance for Server Security

Microsoft. Windows Server 2003 Security Guide.

Microsot. Security Templates. http://go.microsoft.com/fwlink/?LinkId=14846