Microsoft® Official Academic Course

Fundamentos de Seguridad

EXAMEN 98-367

WILEY

Índice

1. Capas de Seguridad 1
2. Autenticación, Autorización y Auditoría 25
3. Directivas de Seguridad 83
4. Seguridad en la Red 105
5. Cómo Proteger al Servidor y al Cliente 159

Contenido

Lección 1
Capas de Seguridad 1

Introducción a la Seguridad 2
- Qué es la confidencialidad 2
- Qué es Integridad 3
- Qué es Disponibilidad 3
- Amenazas y Administración de Riesgos 3
- Principio de Privilegio Mínimo 6
- Superficie de Ataque 7
- Qué es la Ingeniería Social 8
- Vinculación del Costo con la Seguridad 9

Tomar en Cuenta la Seguridad Física como la Primera Línea de Defensa 10
- Comprender la Seguridad del Sitio 10
  - Comprender el Control de Acceso 10
  - Comprender la Seguridad del Perímetro Exterior 12
  - Comprender el Perímetro Interno 13
  - Definición de las Áreas Seguras 13
  - Procesos de Seguridad del Sitio 14
- Seguridad Informática 14
  - Entender la Seguridad de los Dispositivos Portátiles 15
  - Dispositivos y Discos Extraíbles 16
  - Keyloggers 18

Evaluación de Conocimientos 20
Entendiendo lo Básico 22
Evaluación de Competencia 23
Evaluación de Habilidad 23

Lección 2
Autenticación, Autorización y Auditoría 25

Seguridad al iniciar con Autenticación 26
- Autenticación mediante algo que se sabe 26
  - Contraseñas 26
  - Número de Identificación Personal (PIN) 28
- Autenticación por medio de algo que se posee 28
- Autenticación demostrando quién se es 29
- Introducción a RADIUS y TACACS+ 29
- Ejecutar Como 30
- Ejecutar un programa como administrador 30

Introducción a los Servicios de directorio utilizando Directorio activo (Active Directory) 31
- Análisis de los controladores de dominio 32
- Introducción a NTLM 33
- Introducción a Kerberos 33
- Unidades organizacionales 34
- Análisis de los objetos 35
  - Examinar los usuarios 36
  - Análisis de los equipos 37
- Qué son los grupos 38
  - Examen de los tipos de grupos 38
  - Examen de los alcances del grupo 38
  - Grupos integrados 40
- Buscar la autenticación del servidor Web 40

Comparar los derechos y permisos 41
Análisis de NTFS 42
En Resumen 42
- Permisos de NTFS 42
- Permisos efectivos de NTFS 44
- Copiar y mover archivos 47
- Propietario de carpeta y archivos 48
- Hacer uso de un archivo o carpeta 48

Hacer uso compartido de unidades y carpetas 49
- Recursos Administrativos Compartidos Especiales 51

Introducción al Registro 51
En Resumen 51
Hacer uso del encriptado para proteger los datos 54

- Examen de los tipos de encriptado 55
  - Análisis del encriptado simétrico 55
  - Análisis del encriptado asimétrico 56
  - Análisis de la función Hash 56
- Introducción a la infraestructura de clave pública 57
  - Certificados digitales 58

Examen de una cadena de certificados (Certificate Chain) 60
Firma Digital 60
Protocolo de Capa de Conexión Segura (SSL) y Seguridad de la Capa de Transporte (TLS) 61
Codificar el Correo Electrónico 62
Encriptar archivos con EFS 62
Encriptar discos de Windows 65
Habilitar BitLocker 66
BitLocker y agentes de recuperación de datos 68
BitLocker To Go 69
Introducción a IPsec 69
Encriptado con tecnología VPN 70
Auditoría para Completar el cuadro de Seguridad 73
En Resumen 73
Evaluación del conocimiento 78
Evaluación de Competencias 81
Evaluación de Habilidades 81
Planificación y mantenimiento de la seguridad 82

Lección 3
Directivas de Seguridad 83

Directivas sobre Contraseñas para Mejorar la Seguridad 84
En Resumen 84
El nivel de Complejidad de una Contraseña para hacerla más fuerte 84
Bloqueo de Cuenta para evitar el Hacking 85
Longitud de Contraseña 86
Historial de Contraseñas para Mantener la Seguridad 86
Tiempo entre Cambios de Contraseñas 86
Directivas de Grupo sobre Contraseñas para Mantener la Seguridad 93
Los Métodos de Ataque Comunes 96
Análisis de Ataques mediante un Diccionario y con Fuerza Bruta 96
Ataques Físicos 97
Contraseñas Divulgadas sin Autorización y Compartidas 97
Contraseñas Crackeadas 98
Examen de Sniffers de Red e Inalámbricos 98
Contraseñas Adivinadas 99
Evaluación de Conocimientos 100
Evaluación de Competencia 102
Evaluación de Habilidad 103
Directivas de Grupo 103

Lección 4
Seguridad en la Red 105

Utilizar Cortafuegos (firewalls) dedicados para proteger una Red 106
En Resumen 106
Comprensión del Modelo OSI 107
Análisis de Firewalls de Hardware y sus Características 110
Análisis del filtrado de paquetes 111
Análisis de los cortafuegos a nivel de circuito 112
Análisis de los cortafuegos a nivel de aplicación 112
Análisis de los cortafuegos con estado Multinivel 113
Cortafuegos de hardware contra cortafuegos de software 113
Inspección Stateful contra la Inspección Stateless 115
Controlar el acceso con la Protección de Acceso a Redes (NAP) 116
En Resumen 116
El propósito de la NAP 116
Cómo funciona la NAP 117
Requisitos para la NAP 120
Usar el aislamiento para proteger la red 121
En Resumen 121
LAN virtuales 121
Qué es el enrutamiento 123
Cómo funciona el enrutamiento 125
Protocolos de enrutamiento 126
Sistemas de Prevención y Detección de Intrusión 128
Qué son los Honeypots 129
Qué son las DMZ 131
Traducción de Dirección de Red (NAT) 133
Redes Privadas Virtuales (VPN) 134
Internet Protocol Security (IPsec) 135
Otros Protocolos VPN 137
Utilizar el Protocolo de Capa de Conexión Segura (SSL) y Seguridad de la Capa de Transporte (TLS) 137
Secure Shell (SSH) 138
Aislamiento del Dominio y del Servidor 139

Proteger los datos con la seguridad del protocolo 141
En Resumen 141
Qué es el Túnel 141
Extensiones de Seguridad del DNS (DNSSEC) 142
Protocol Spoofing 143
Sniffing de Red 143
Métodos Comunes de Ataque a la red 145
Asegurar Redes Inalámbricas 148
En Resumen 148
Service Set Identifier (SSID) 149
Comprender las Claves 149
Wired Equivalency Privacy (WEP) 149
Acceso Protegido Wi-Fi (WPA) y Acceso Protegido Wi-Fi Versión 2 (WPA2) 150
Filtros MAC 151
Pros y Contras de tipos de seguridad específicos 151
Evaluación de Conocimientos 154
Evaluación de competencias 157
Evaluación de Habilidades 157
Estación de trabajo lista 158
Defensa a Profundidad 158

Lección 5
Cómo proteger al Servidor y al Cliente 159

Cómo proteger la computadora cliente 160
En Resumen 160
Cómo proteger su computadora de Malware 160
Tipos de Malware 160
Cómo Identificar Malware 162
Actualizaciones de Seguridad y Software de Antivirus para los Clientes 163
Cómo Usar el Sentido Común con el Malware 163
Cómo eliminar Malware 164
Cómo examinar un Virus Hoax 165
Cómo utilizar Windows Updates 165
Control de Cuenta de Usuario (UAC) 168
Usar el Firewall de Windows 172
Usar Archivos Offline 175
Bloquear la computadora de un Cliente 176
Cómo Proteger Su Correo Electrónico 177
En Resumen 177
Tratar con el Spam 177
Transferencia de Correos Electrónicos 179
Cómo Asegurar Internet Explorer 179
En Resumen 179
Cookies y Configuraciones de Seguridad 179
Cómo Examinar las Zonas de Contenido 182
Phishing y Pharming 185
Cómo Proteger Su Servidor 186
En Resumen 186
Cómo Colocar el Servidor 186
Cómo Fortalecer al Servidor 186
Cómo Asegurar DNS Dinámico 188
Evaluación de Conocimiento 190
Evaluación de Competencia/Capacidad 193
Evaluación de Destreza 193
Cómo Mantener el Paso con la Seguridad 194

Lección 1

Capas de Seguridad

Matriz para la Lección sobre Capacidad

Capacidad Tecnológica	Dominio del Objetivo	Número del Dominio Objetivo
Introducción a la Seguridad	Comprender los principios básicos de seguridad.	1.1
Análisis de la Seguridad Física como la Primera Línea de Defensa	Comprender la seguridad física.	1.2

Términos clave

- Control de acceso
- Superficie de ataque
- Disponibilidad
- Confidencialidad
- Defensa en profundidad
- Unidad flash (Flash drive)
- Integridad
- Capturador de teclado (keylogger)
- Dispositivo móvil
- Principio de privilegio mínimo
- Dispositivo extraíble
- Riesgo residual
- Riesgo
- Aceptación del riesgo
- Evaluación de riesgo
- Prevención de riesgo
- Gestión de riesgo
- Mitigación de riesgo
- Transferencia de riesgo
- Ingeniería social
- Amenaza

Cuando pensamos en seguridad, podemos comenzar por tomar en cuenta nuestras cosas personales. Todos tenemos objetos que realmente nos importan, unos que serían difíciles de reemplazar y otros que tienen un gran valor sentimental. Tenemos cosas de las que no queremos que otras personas se enteren, incluso algunas sin las cuales tampoco podríamos vivir. Piense ahora en donde las guarda. Podría ser en su casa, automóvil, escuela u oficina; en un locker, en una mochila o maleta o en otros numerosos lugares. Piense en todo lo malo que podría ocurrirle a sus cosas. Puede ser asaltado o encontrarse en un desastre natural por ejemplo un incendio, un terremoto o una inundación. De cualquier manera desea proteger sus posesiones, sin importar de donde proviene la amenaza.

A un alto nivel, la seguridad es para proteger algo. En el caso de las cosas personales, se trata de asegurarse que cierra con llave la puerta al salir de la casa, acordarse de llevar consigo la bolsa al salir de un restaurant o incluso asegurarse que ha escondido en la parte trasera de su automóvil todos los regalos que compró para los días de fiesta antes de regresar a la plaza comercial.

Muchos de los temas de seguridad acerca de los que hablaremos en esta lección se reducen al mismo sentido común que utilizamos todos los días para proteger nuestras cosas. En el entorno empresarial, sin embargo, lo que estamos protegiendo son recursos, información, sistemas y redes, y podemos proteger estos objetos de valor mediante una variedad de herramientas y técnicas sobre las cuales hablamos en detalle en este libro.

En esta lección, comenzamos por lo básico. Analizaremos algunos de los principios básicos de un programa de seguridad y así establecer la base para la comprensión de los temas más avanzados que se verán más adelante en este libro. También hablaremos acerca del concepto de seguridad física, la cual es esencial no únicamente para asegurar los recursos físicos, sino también los recursos de información. Cuando terminemos, tendrá una buena idea de cómo proteger efectivamente las cosas necesarias en todos los aspectos de la vida.

▪ Introducción a la Seguridad

↓ EN RESUMEN

Antes de empezar a asegurar su entorno, es necesario tener una comprensión fundamental de los conceptos estándar de seguridad. Es fácil comenzar a comprar firewalls, pero hasta que entienda qué es lo que trata de proteger, por qué necesita estar protegido y de qué lo está protegiendo, únicamente está tirando su dinero a la basura.

☑ Listo para la Certificación

¿Puede enumerar y describir lo que representa CIA en lo que se refiere a seguridad? —1.1

Cuando se trabaja en el campo de seguridad de la información, una de las primeras siglas con las que nos encontraremos es CIA – pero no hay que confundirlas con la agencia gubernamental con las mismas siglas. Más bien, en este contexto, CIA representa los objetivos básicos de un programa de seguridad de la información:

- Confidencialidad
- Integridad
- Disponibilidad

▶ *Qué es la confidencialidad*

Confidencialidad es un concepto con el que tratamos con frecuencia en la vida real. Por ejemplo, esperamos que nuestros médicos mantengan nuestros expedientes como confidenciales y confiamos en que nuestros amigos mantengan nuestros secretos como confidenciales. En el mundo de los negocios, definimos la confidencialidad como la característica de un recurso que asegura que el acceso está restringido para ser utilizado únicamente por usuarios, aplicaciones o sistemas informáticos autorizados. Pero, ¿qué significa esto en realmente? En pocas palabras, la confidencialidad se ocupa de mantener la información, las redes y los sistemas seguros frente a cualquier acceso no autorizado.

Referencia Cruzada

La Lección 2 contiene más detalles acerca de una encriptación de alta seguridad, una fuerte autenticación y estrictos controles de acceso

La confidencialidad es particularmente crítica en el entorno actual. Recientemente, en algunos casos de alto perfil, diversas empresas importantes han filtrado información personal de algunos individuos. Estas violaciones de la confidencialidad estuvieron en las noticias en gran parte debido a que la información filtrada podría ser utilizada para llevar a cabo el robo de identidad de las personas cuya información había sido diseminada.

Existen varias tecnologías que apoyan la confidencialidad en la implementación de seguridad en una empresa. Estas incluyen:

- Una encriptación de alta seguridad
- Una fuerte autenticación
- Estrictos controles de acceso

★ Tome Nota

Clasifique su información y sus activos (es la única manera en que puede protegerlos eficazmente)

Otro componente clave que se debe de tomar en consideración al hablar de la confidencialidad es cómo determinar qué información es considerada como privada. Algunas clasificaciones comunes de la información son "Pública", "Únicamente para Uso Interno", "Confidencial (o privada)" y "Estrictamente Confidencial". También podrá observar la clasificación "Privilegiado", la cual es utilizada con frecuencia entre abogados. De la misma manera, los militares muchas veces clasifican la información como "No Clasificada", "Restringida", "Confidencial". "Secreta" o "Ultra Secreta". Estas clasificaciones son utilizadas para determinar las medidas apropiadas para proteger la información. Si su información no es clasificada, tendrá dos opciones, puede proteger toda su información como si fuera confidencial (una tarea costosa y de enormes proporciones) o puede tratar toda su información como si fuera "Pública" o "Únicamente para Uso Interno" y no tomar medidas estrictas de protección.

Qué es Integridad

En el contexto de seguridad de la información, la ***integridad*** es definida como la consistencia, la precisión y la validez de los datos y la información. Uno de los objetivos de un programa exitoso de seguridad para la información, es asegurar que la información esté protegida frente a cualquier cambio no autorizado o accidental. Por lo tanto, un programa de seguridad debe incluir procesos y procedimientos para manejar cambios intencionales, así como la capacidad para detectar cambios. Algunos de los muchos procesos que se pueden utilizar para asegurar eficazmente la integridad de la información incluyen la autenticación, la autorización y la auditoría. Por ejemplo, puede utilizar derechos y autorizaciones para controlar quién puede tener acceso a cierta información o recursos. También puede utilizar una función Hash (una función matemática) que puede ser calculada con relación a la información o a un mensaje antes y después de un periodo determinado de tiempo para mostrar si la información ha sido modificada durante ese tiempo en específico o puede utilizar un sistema de auditoría o trazabilidad que registra cuando se han producido cambios.

Qué es Disponibilidad

Disponibilidad es el tercer principio básico de la seguridad y describe un recurso que es accesible para un usuario, una aplicación o sistema informático cuando es requerido. En otras palabras, disponibilidad significa que cuando un usuario necesita obtener información, él o ella tienen la capacidad de obtenerla.

Por lo general, las amenazas a la disponibilidad son de dos tipos: accidental y deliberada. Las amenazas accidentales incluyen desastres naturales tales como tormentas, inundaciones, incendios, cortes de energía eléctrica, terremotos, etc. Esta categoría también incluye cortes debidos a fallas en el equipo, problemas de software y otros problemas no planeados relacionados con el sistema, la red o el usuario. La segunda categoría (amenazas deliberadas) relacionadas con cortes que son el resultado de la explotación de una vulnerabilidad del sistema. Algunos ejemplos de este tipo de amenaza incluyen ataques de denegación de servicio o gusanos informáticos que afectan a los sistemas vulnerables y su disponibilidad. En algunos casos, una de las primeras acciones que deberá tomar después de un corte, es determinar la categoría de éste. Las empresas manejan las interrupciones accidentales de manera muy diferente a las interrupciones deliberadas.

Amenazas y Administración de Riesgos

La administración de riesgos es el proceso mediante el cual se identifica, evalúa y se da prioridad a las amenazas y los riesgos. Un ***riesgo*** es definido generalmente como la probabilidad de que ocurra un evento. En la realidad, las empresas sólo están preocupadas por los riesgos que podrían tener un impacto negativo sobre el entorno informático. Por ejemplo, existe una probabilidad de que pudiera ganar la lotería el viernes, pero esto no es un riesgo que su empresa aborde de manera activa, porque sería algo positivo. Más bien, su empresa podría estar más preocupada por el tipo específico de riesgo que se conoce como una ***amenaza***, el cual es definido como una acción o suceso que pudiese resultar en la violación, corte o corrupción de un sistema mediante la explotación de vulnerabilidades conocidas o desconocidas. Generalmente, cuando alguien se refiere a la administración de riesgos, se está enfocando en este tipo de riesgo negativo. El objetivo de cualquier plan de administración de riesgos es el de eliminar las amenazas siempre que esto sea posible y el de minimizar las consecuencias de las que no pueden ser eliminadas. El primer paso para la creación de un plan para la administración de riesgos es llevar a cabo una ***evaluación.*** Las evaluaciones de riesgos generalmente se utilizan para identificar los peligros que pudieran tener un impacto sobre un entorno en particular.

Tome Nota

En un entorno desarrollado de evaluación de riesgos es común registrarlos, debido a que su oportuna documentación proporciona un mecanismo formal para revisar sus impactos, controles y cualquier otra información requerida por el programa de administración de riesgos.

Una vez que ha terminado su evaluación e identificado sus riesgos, es necesario que valore cada riesgo en busca de dos factores; primero, debe determinar la probabilidad de que un riesgo pudiese ocurrir en su entorno, por ejemplo, es mucho más probable que un tornado ocurra en Oklahoma que en Vermont. No es muy probable que caiga un meteorito en algún lugar, sin embargo, es un ejemplo que se utiliza comúnmente para representar la pérdida total de una instalación, al hablar de riesgos. Una vez que ha determinado la probabilidad de un riesgo específico, debe determinar el impacto que ese riesgo tendría sobre su entorno. Por ejemplo, un virus en la estación de trabajo de un usuario generalmente tiene poco impacto sobre la empresa (aún cuando sí constituye un alto impacto para el usuario). Un virus en su sistema financiero tiene un impacto general mucho mayor, aunque se espera que sea una probabilidad mucho menor.

Una vez que ha evaluado sus riesgos, llega el momento de darles una prioridad. Uno de los mejores mecanismos para ayudarle a establecer prioridades, es la creación de una matriz de riesgos, la cual puede ser utilizada para determinar una clasificación de amenaza global. Una matriz de riesgos debe incluir los siguientes elementos:

- El riesgo
- La probabilidad de que realmente ocurra el riesgo
- El impacto del riesgo
- Una puntuación total de riesgo
- El dueño del proceso afectado (persona, equipo o departamento) por el riesgo
- Los principios de seguridad básicos afectados por el riesgo, confidencialidad, integridad y/o disponibilidad.
- La estrategia o estrategias apropiadas para hacer frente al riesgo.

Algunos campos adicionales que podrían ser de utilidad en su registro de riesgos son los siguientes:

- Una fecha cuando el riesgo que debe ser abordado
- Documentación con relación al riesgo residual (p. ej., el riesgo que queda después de que se han tomado las medidas para reducir la probabilidad o minimizar el efecto de un evento).
- El estatus de la estrategia o estrategias que se utilizan para abordar el riesgo; esto puede incluir indicadores tales como “Planeación” “en Espera de Aprobación”, “Implementación” y “Completo”.

Una forma sencilla para calcular una puntuación total de riesgo es la de asignar valores numéricos a su probabilidad e impacto. Por ejemplo, puede clasificar la probabilidad y el impacto sobre la base de una escala de 1 al 5, donde 1 equivale a una baja posibilidad y 5 equivale a un alto impacto. A continuación, puede multiplicar en conjunto la probabilidad y el impacto para generar una puntuación total de riesgo. Mediante la clasificación de mayor a menor, cuenta con un método fácil para dar una prioridad inicial a sus riesgos. A continuación, debe repasar los riesgos específicos para determinar el orden final en que desea abordarlos. En este punto, es posible que se encuentre con factores externos, tales como costos o recursos disponibles, que afecten sus prioridades.

Una vez que ha dado prioridad a sus riesgos, está listo para elegir entre las cuatro respuestas generalmente aceptadas para éstos. Estas incluyen:

- Evitar
- Aceptar
- Mitigar
- Transferir

Evitar riesgos es el proceso de eliminar una probabilidad al optar por no participar en una acción o actividad. Un ejemplo de evitar riesgos es cuando una persona que sabe que existe una posibilidad de que el valor de una acción pudiera caer, decide evitar el riesgo al no comprar la acción. Un problema que surge cuando evitamos un riesgo es que con frecuencia hay una recompensa asociada al mismo, por lo tanto, si evita el riesgo, también está evitando la recompensa. Por ejemplo, si la acción en el ejemplo anterior fuese a triplicar su precio, el inversionista con aversión al riesgo perdería la recompensa debido a que quiso evitarlo.

Aceptar riesgos es el acto de identificar, para posteriormente tomar una decisión informada de aceptar la probabilidad y el impacto de un riesgo específico. Para utilizar nuevamente el ejemplo de la actividad, el aceptar riesgos es el proceso mediante el cual un comprador analiza cabalmente a una empresa en cuyas acciones está interesado y después de considerar esta información, toma la decisión de aceptar el riesgo de que pudiese caer el precio de esta.

Mitigar el riesgo consiste en tomar medidas para reducir la probabilidad o el impacto de un riesgo. Un ejemplo común de mitigación es el uso de discos duros redundantes en un servidor. En todos los sistemas existe el riesgo de una falla del disco duro. Mediante el uso de una arquitectura de matriz redundante de discos, puede mitigar el riesgo de una falla en una de las unidades al tener un disco de respaldo. En otras palabras, aunque cuando el riesgo continúa existiendo, sus acciones lo han reducido.

Transferir el riesgo es el acto de tomar medidas para pasar la responsabilidad por un riesgo a un tercero mediante un seguro o una subcontratación. Por ejemplo, existe un riesgo que pueda sufrir un accidente al estar conduciendo su automóvil. Así, transfiere ese riesgo al adquirir un seguro, de manera que en caso de un accidente, su compañía de seguros es la responsable por pagar la mayoría de los costos relacionados con el accidente.

Como se mencionó anteriormente, otro concepto importante en la administración de riesgos es el ***riesgo residual.*** El riesgo residual es la amenaza que queda después de que se han tomados medidas para reducir la probabilidad o minimizar el efecto de un evento en particular. Para continuar con el ejemplo del seguro del automóvil, su riesgo residual en el caso de un accidente sería el deducible que debe pagar antes que su compañía aseguradora se haga cargo de la responsabilidad por el resto del daño.

Tome Nota

Existen muchas diferentes maneras para identificar, evaluar y dar prioridad a los riesgos. No existe una manera correcta. Utilice las técnicas que mejor se adapten a su entorno y sus necesidades.

Ahora, como parte de nuestro análisis de riesgo, también debemos de tener en cuenta dos conceptos finales que le ayudarán a entender los fundamentos de los principios de seguridad y de administración de riesgos: el principio de mínimo privilegio, y la idea de una superficie de ataque.

Principio de Privilegio Mínimo

El *principio de privilegio mínimo* es una disciplina de seguridad que requiere que un usuario, un sistema o una aplicación en particular no reciba más privilegio que el necesario para llevar a cabo su función o su trabajo. Esto suena como un enfoque con sentido común para asignar autorización, y cuando se ve en el papel, así es. Sin embargo, cuando se comienza a aplicar este principio en un entorno de producción complejo, se vuelve mucho más difícil.

El principio de privilegio mínimo ha sido un elemento básico en el campo de la seguridad durante varios años, y muchas organizaciones han tenido dificultades para implementarlo con éxito. Sin embargo, con el mayor enfoque hacia la seguridad que existe en la actualidad, tanto desde el punto de vista comercial como regulatorio, las empresas se están esforzando más arduamente que nunca para construir sus modelos en torno a este principio. Los requisitos reglamentarios de Sarbanes-Oxley, HIPAA, HITECH y diversos reglamentos estatales, aunados a un mayor enfoque hacia las prácticas de seguridad de sus socios de negocio, proveedores y consultores están impulsando a las empresas a invertir en herramientas, procesos y otros recursos para garantizar el cumplimiento de este principio.

¿Pero por qué un principio que parece tan sencillo en el papel es tan difícil de implementar en la práctica? El reto está relacionado principalmente con la complejidad el entorno típico de trabajo. Es fácil visualizar la aplicación del principio de privilegio mínimo para un solo empleado. Sobre una base física, el empleado necesita tener acceso al edificio donde trabaja, a cualquier área común y a su oficina. Lógicamente, el empleado también necesita poder iniciar sesión en su computadora, tener acceso a algunas aplicaciones centralizadas y tener acceso a un servidor de archivos, una impresora y un sitio web interno. Ahora imagine a ese usuario multiplicado por mil e imagine que todos esos empleados trabajan en seis oficinas diferentes. Algunos necesitan tener acceso a las seis oficinas, mientras que otros únicamente necesitan tener acceso a su propia oficina. Otros más necesitan tener acceso a subconjuntos específicos en las seis ubicaciones; por ejemplo, es posible que requieran tener acceso a las dos oficinas en su región, o tal vez requieran tener acceso a los centros de datos para poder proporcionar soporte de TI.

En esta situación, en lugar de un solo conjunto de requisitos de acceso, ahora cuenta con múltiples departamentos con diferentes requisitos de aplicación. También tiene diferentes tipos de usuarios, que varían desde usuarios "regulares" hasta usuarios avanzados para los administradores; por lo tanto, debe determinar, no únicamente el tipo de usuario que es cada empleado, sino también cuáles son las aplicaciones internas a los cuales tendrá acceso. A esta mezcla deben agregarse nuevas contrataciones, empleados que son transferidos o ascendidos y empleados que salen de la empresa, y puede comenzar a darse cuenta cómo asegurarse que cada empleado cuente con la mínima cantidad de acceso que requiere para desempeñar su trabajo, puede ser una actividad que consume mucho tiempo.

Pero espere, no hemos acabado. Además de las autorizaciones físicas y de usuario, también debe de ser consciente que en muchos entornos de TI, ciertas aplicaciones requieren de acceso a datos y/u otras aplicaciones. Por lo tanto, para cumplir con el principio de privilegio mínimo, debe asegurarse que estas aplicaciones cuenten con el mínimo acceso necesario para funcionar adecuadamente. Esto puede ser sumamente difícil cuando se trabaja en un entorno de Microsoft Active Directory, debido a la detallada autorización incluida en él. El determinar qué autorizaciones requiere una aplicación para funcionar adecuadamente con Active Directory puede ser un gran reto.

Para complicar aún más las cosas, en industrias en las cuales hay una intensa regulación, como por ejemplo en los ámbitos médicos o financieros, o cuando las regulaciones como Sarbanes-Oxley están en vigor, hay requisitos adicionales que estipulan que se debe llevar

regularmente una auditoría para asegurar que se han implementado con éxito y se han validado privilegios en toda la empresa.

★ Tome Nota

Una perfecta implementación del principio de privilegio mínimo es muy poco común. Típicamente, lo que se puede esperar es el mejor esfuerzo y lo que sea posible lograr

Una explicación detallada acerca de cómo implementar y mantener el principio de privilegio mínimo está más allá del alcance de este libro, pero hay algunas herramientas y estrategias de alto nivel de las cuales debemos ser conscientes, incluyendo las siguientes:

Grupos: Los grupos nos permiten concentrar lógicamente a los usuarios y las aplicaciones de manera que las autorizaciones no sean empleadas sobre una base de usuario por usuario o aplicación por aplicación.

- **Múltiples cuentas de usuarios para los administradores:** Los administradores son uno de los mayores retos en la implementación del principio de privilegio mínimo. Generalmente, los administradores también son usuarios, y muy pocas veces es una buena idea que lleven a cabo sus tareas diarias como un administrador. Para hacer frente a este problema, muchas empresas emiten dos cuentas para sus administradores, una para su papel como usuario de las aplicaciones y sistemas de la empresa, y el otro para su papel de administrador.
- **Estandarización de cuentas:** La mejor manera de simplificar un entorno complejo es la de estandarizar un número limitado de tipos de cuenta. Cada diferente tipo de cuenta permitido en su entorno agrega un orden de magnitud a su estrategia de gestión de autorizaciones. El estandarizar un conjunto limitado de tipos de cuenta, hace que su trabajo sea más fácil.
- **Aplicaciones de terceros:** Ha sido diseñada una variedad de herramientas de terceros para hacer más sencilla la administración de autorizaciones. Éstas van desde aplicaciones para la administración del ciclo de vida, hasta aplicaciones de auditoría, hasta aplicaciones de firewalls.

▶ *Superficie de Ataque*

Un concepto final que se debe enfrentar al evaluar la seguridad de nuestro entorno es el de una ***superficie de ataque***. Con respecto a sistemas, redes y aplicaciones, ésta es otra idea que ha existido desde hace bastante tiempo. Una superficie de ataque consiste en un conjunto de métodos y vías que un atacante puede utilizar para penetrar a un sistema y, potencialmente, ocasionar daños. Entre mayor sea la superficie de ataque de un entorno en particular, mayor será el riesgo de un ataque exitoso.

Para calcular la superficie de ataque de un entorno, a menudo, la forma más sencilla es la de dividir la evaluación en tres componentes:

- Aplicación
- Red
- Empleado

Al evaluar la superficie de ataque de una aplicación, es necesario observar cosas tales como:

- La cantidad de código en una aplicación
- El número de entradas de datos en una aplicación
- El número de servicios en ejecución
- Los puertos que la aplicación está escuchando

De la misma manera, al evaluar la superficie de ataque de la red, debemos tomar en consideración lo siguiente:

- Diseño general de la red
- Colocación de los sistemas críticos

- Colocación y conjuntos de reglas en los firewalls
- Otros dispositivos de seguridad relacionados con la red, tales como IDS, VPN, etc.

Finalmente, al evaluar la superficie de ataque del empleado, debemos tomar en consideración los siguientes factores:

- El riesgo de la ingeniería social
- La posibilidad de errores humanos
- El riesgo de un comportamiento malicioso

Una vez evaluados estos tres tipos de superficie de ataque, contaremos con una sólida comprensión del total de las superficies de ataque presentadas por su entorno, así como la manera en que un atacante podría tratar de poner en peligro su entorno.

Qué es la Ingeniería Social

Como ya hemos mencionado anteriormente, uno de los factores clave que se debe de tomar en consideración al evaluar la superficie de ataque de un empleado es el riesgo de un ataque de ingeniería social. La ***ingeniería social*** es un método utilizado para obtener acceso a datos, sistemas o redes, principalmente a través de falsificaciones. Está técnica está basada típicamente en la naturaleza confiada de la persona que está siendo atacada.

En un ataque de ingeniería social típico, el atacante tratará de parecer lo más inofensivo o respetuoso posible. Estos ataques pueden ser perpetrados en persona, por medio del correo electrónico o por vía telefónica. Los atacantes intentarán diversas técnicas, desde pretender ser un servicio de asistencia o un empleado del departamento de soporte técnico, diciendo que es un nuevo empleado, o, en algunos casos, hasta llegan a presentar una credencial que los identifica como empleado de la empresa.

Generalmente, estos atacantes harán una serie de preguntas en un intento por identificar posibles vías que puedan ser explotadas durante un ataque. En caso que no reciba suficiente información de un empleado, pueden ponerse en contacto con otros empleados, hasta contar con la información suficiente para la siguiente fase de un ataque.

Para evitar los ataques de ingeniería social, recuerde las siguientes técnicas:

- **Desconfíe:** Llamadas telefónicas, correos electrónicos o visitantes que hacen preguntas acerca de la empresa, sus empleados u otra información interna deben ser tratados con extrema desconfianza, y en caso de ser apropiado, reportados al personal de seguridad.
- **Verifique la identidad:** Si recibe consultas acerca de las cuales no está seguro, verifique la identidad del solicitante. Si una persona que llama por teléfono hace preguntas que parecen extrañas, intente obtener su número telefónico para devolver la llamada. A continuación, verifique que el número telefónico que le han proporcionado procede de una fuente legítima. De la misma manera, si alguien se le acerca con una tarjeta de presentación como identificación, solicite que le muestre una identificación con fotografía. Es muy sencillo imprimir tarjetas de presentación, y son aún más sencillas de obtener tomándolas del tazón de "Gane una Comida Gratis" en un restaurante local.
- **Sea cauteloso:** No proporcione información confidencial a menos que esté seguro, no únicamente de la identidad de la persona, sino también de su derecho de poseer la información.
- **No utilice el correo electrónico:** El correo electrónico es inherentemente poco seguro y propenso a una variedad de técnicas de suplantación de direcciones. Por lo tanto, no revele información personal o financiera mediante un correo electrónico

(sea particularmente cauteloso al proporcionar esta información después de seguir enlaces a la web incorporados en un correo electrónico). Un truco muy común es el de incorporar un el enlace de búsqueda en un correo electrónico, posiblemente ofreciendo un premio o participación en una rifa y a continuación haciendo preguntas acerca del entorno informático tales como "¿Cuántos firewalls ha implementado?" o "¿Qué proveedor de firewall usa?" Los empleados están tan acostumbrados a ver este tipo de peticiones de encuesta en su bandeja de entrada, que rara vez piensan dos veces antes de responder a ellas.

Tome Nota

La clave para frustrar un ataque de ingeniería social es la concientización de los empleados. Si sus empleados saben de lo que se deben cuidar, un atacante tendrá muy poco éxito.

▶ *Vinculación del Costo con la Seguridad*

Hay algunos puntos que debemos tener en cuenta al desarrollar un plan de seguridad. Primero, la seguridad cuesta dinero. Por lo general, entre más dinero se gasta, más segura estará nuestra información o nuestros recursos (hasta cierto punto). Por la tanto, al analizar los riesgos y las amenazas, debemos tomar en consideración qué tan valiosa es cierta información o recursos confidenciales para la empresa y cuánto dinero estamos dispuestos a gastar para proteger esa información o recursos.

Además de tomar en consideración el costo, también deberá esforzarse para que las medidas de seguridad sean lo más sencillas posibles para los usuarios autorizados que tienen acceso a la información o el recurso confidencial. Si la seguridad se convierte en una carga pesada, los usuarios a menudo buscarán métodos para eludir las medidas que ha establecido. Por supuesto, la capacitación es un gran adelanto para proteger su información y recursos confidenciales, porque le muestra a los usuarios cuáles son las señales de alerta a las que deben prestar atención.

▪ Tomar en Cuenta la Seguridad Física como la Primera Línea de Defensa

↓ EN RESUMEN

Hay una serie de factores que se deben tomar en consideración al diseñar, implementar o revisar las medidas de seguridad físicas que se han tomado para proteger los activos, los sistemas, las redes y la información. Estos incluyen, entender la seguridad del sitio y la seguridad informática; asegurar las unidades y dispositivos extraíbles; controlar el acceso; la seguridad de dispositivos móviles; deshabilitar la capacidad para Inicio de Sesión Local, y la identificación y remoción de los keyloggers.

☑ Listo para la Certificación

¿Por qué es tan importante la seguridad física para un servidor, aún cuando se necesita de nombres de usuario y contraseñas para tener acceso a él?

—1.2

La mayoría de los negocios ejercen algún nivel de control sobre quién tiene derecho a tener acceso a su entorno físico. Al asegurar activos y datos relacionados con la informática, hay una tendencia de ver únicamente el mundo virtual, prestando poca atención al tema de la seguridad física. Sin embargo, si trabaja para una empresa grande en una ubicación con un centro de datos, podrá ver lectores de tarjetas y/o teclados para acceder al edificio y a cualquier área segura, junto con personal de seguridad y tal vez hasta bitácoras para controlar y rastrear a las personas que entran al edificio. Las llaves de la oficina y las llaves del cajón del escritorio proporcionan otra capa más de seguridad. En las oficinas más pequeñas, pueden existir medidas similares, aunque en menor escala.

Tome Nota

En caso que alguien obtenga acceso a un servidor en el cual se almacenan datos confidenciales, si cuenta con las herramientas apropiadas y el tiempo suficiente, esa persona puede eludir cualquier seguridad utilizada por el servidor para proteger la información.

Este enfoque de varias capas para la seguridad física es conocido como defensa en profundidad o enfoque de seguridad por capas. Asegurar un lugar físico es más que únicamente colocar una cerradura en la puerta de adelante y asegurarse de utilizar esa cerradura. Más bien, es un reto muy complejo para cualquier profesional de la seguridad.

Tome Nota

La seguridad no termina con la seguridad física. También es necesario proteger la información confidencial mediante tecnología basada en la autenticación, la autorización y la auditoría – incluyendo el uso de derechos, permisos y encriptado.

▶ *Comprender la Seguridad del Sitio*

La seguridad del sitio es un área especializada de la disciplina de la seguridad. El propósito de esta sección es el de introducir algunos de los conceptos y tecnología más comunes con las que nos podemos encontrar al trabajar en el campo de la seguridad.

Comprender el Control de Acceso

Antes de entrar en detalle en la seguridad del sitio, primero debe comprender lo que significa el término "control de acceso". El ***Control de acceso*** es un concepto clave al pensar en la seguridad física. También es un poco confuso, ya que frecuentemente escuchará la frase cuando se habla de seguridad de la información. En el contexto de la seguridad física,

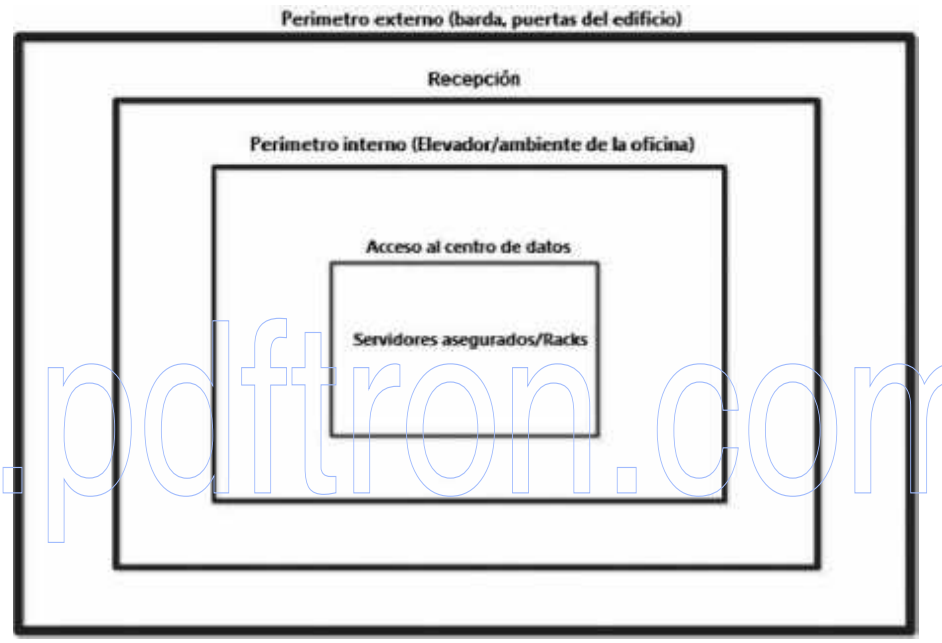
es el proceso de restringir el acceso a un recurso siendo éste únicamente para los usuarios autorizados, aplicaciones o sistemas informativos.

Si lo piensa bien, probablemente podrá dar varios ejemplos cotidianos de control de acceso. Por ejemplo, cuando cierra una puerta y le echa llave, está llevando a cabo uno. Cuando utiliza una reja para bebé y así evitar que se caiga por la escalera, está practicando control de acceso. De la misma manera, cuando coloca una barda alrededor de su patio para evitar que el perro pise las flores de su vecino, lo está aplicando.

La diferencia entre el control de acceso que practica en su vida cotidiana y el control de acceso con el que se encontrará en el mundo de los negocios, es la naturaleza de lo que está protegiendo y las tecnologías con las que cuenta para asegurarlo. Veremos estos temas en mayor detalle durante el resto de la lección.

Figura 1-1

Modelo de la seguridad en capas para el sitio



Como ya hemos mencionado, la seguridad del sitio involucra la protección de las instalaciones físicas. Un concepto fundamental que se usa al diseñar un entorno de seguridad es el de la defensa a profundidad. La ***Defensa a profundidad*** significa la utilización de múltiples capas de seguridad para proteger sus activos. De esta manera, aún si un atacante viola una capa de defensa, cuenta con capas adicionales para mantener a esa persona fuera de las áreas críticas de su entorno.

Un sencillo ejemplo de la defensa a profundidad con el que probablemente se ha topado en el "mundo real" es una habitación de hotel que contiene una maleta cerrada con llave. Para entrar a la habitación de hotel, debe introducir su llave. Después de haber llevado a cabo esta tarea, hay un cerrojo que se debe pasar. Y una vez que ha pasado del cerrojo, todavía queda por abrir la cerradura de la maleta.

Más allá de la idea de la defensa a profundidad, existen otros objetivos que se deben tener en mente al diseñar un plan de seguridad física:

- **Autenticación:** La seguridad del sitio debe abordar la necesidad de identificar y autenticar a las personas a quienes se les permite el acceso a un área.

- **Control de Acceso:** Una vez que se ha comprobado y autenticado la identidad de una persona, la seguridad del sitio debe determinar cuáles son las áreas a las que esa persona tiene acceso.
- **Auditoría:** La seguridad del sitio también debe proporcionar la capacidad de auditar las actividades que se llevan a cabo dentro de la instalación. Esto se puede hacer mediante la revisión de los videos de las cámaras, bitácoras de los lectores de tarjetas, bitácoras del registro de visitantes, u otros mecanismos.

Para los fines de esta lección, dividiremos las instalaciones físicas en tres áreas lógicas:

- **El perímetro exterior:** Constituye el área más externa de la instalación. Esto generalmente incluye los caminos de entrada, los estacionamientos y cualquier área verde alrededor de la instalación. Esto no incluye espacios tales como la vía pública.
- **El perímetro interno:** Consiste de cualquier edificio que se encuentre en las instalaciones. Si hay varios inquilinos, su perímetro interno está restringido únicamente a los edificios que ocupa.
- Áreas Seguras: Son las ubicaciones dentro del edificio que cuentan con restricciones de acceso y/o medidas de seguridad adicionales. Estas pueden incluir centros de datos, cuartos para el control de la red, armario de cableado, o departamentos tales como Investigación y Desarrollo o Recursos Humanos.

Comprender la Seguridad del Perímetro Exterior

La seguridad del perímetro exterior es la primera línea de defensa que rodea a su oficina. Sin embargo, las medidas de seguridad en esta área probablemente son las que más varían en comparación con cualquier otro espacio acerca del cual vamos a hablar. Por ejemplo, si está tratando de proteger instalaciones gubernamentales ultra secretas, su parámetro de seguridad del perímetro exterior muy probablemente consistirá de varias bardas, patrullas de vigilancia, minas terrestres y todo tipo de medidas que no se ven en el mundo corporativo. Por otra parte, si su oficina se encuentra en un parque de oficinas que cuenta con múltiples inquilinos, la seguridad del perímetro externo únicamente consistirá de alumbrado público. La mayoría de las empresas están en algún lugar intermedio. Las medidas de seguridad comunes que podrá encontrar con respecto al perímetro externo de una empresa incluyen las siguientes:

- Cámaras de seguridad
- Alumbrado en el estacionamiento
- Barda alrededor del perímetro
- Puerta con vigilancia
- Puerta de acceso con lector de tarjeta de identificación
- Patrullas de vigilancia

Un reto relacionado con las cámaras de seguridad es que estas únicamente son tan buenas como las personas que las están monitoreando. Debido a que las cámaras de monitoreo requieren de un uso intensivo de recursos, en la mayoría de los entornos de oficina no hay ninguna persona que las esté observando activamente. En vez de eso, las cámaras son utilizadas después de que ha ocurrido un incidente, para determinar qué fue lo que sucedió o quién es el responsable.

Tome Nota

Pruebe regularmente la capacidad de reproducción de su cámara. Debido a que casi siempre se utilizan para revisar los eventos después de que han ocurrido, debe estar seguro que su sistema está grabando correctamente toda la información.

Comprender el Perímetro Interno

El perímetro interno de seguridad comienza con las paredes y las puertas exteriores del edificio e incluye todas las medidas de seguridad, a excepción de las áreas seguras dentro del edificio. Algunas de las características que puede utilizar para asegurar un perímetro interno son las siguientes:

- Cerraduras (en puertas exteriores, puertas interiores, puertas de oficina, escritorios, archiveros, etc.)
- Teclados numéricos
- Cámaras de seguridad
- Lectores de tarjetas (en las puertas y los elevadores)
- Escritorios de vigilancia
- Patrullas de vigilancia
- Detectores de humo
- Torniquetes
- Cepos

Las medidas clave de seguridad implementadas en el perímetro interno son aquellas que son utilizadas para dividir el espacio interno en segmentos discretos. Esta es una implementación física del principio de privilegio mínimo. Por ejemplo, si la oficina de una empresa incluye departamentos de finanzas, de recursos humanos y de ventas, no sería poco común el restringir el acceso al departamento de finanzas a únicamente aquellas personas que trabajan en él. Generalmente no se necesita que el personal de recursos humanos esté en el área de finanzas. Estos tipos de segregaciones pueden ser utilizados en los pisos, las áreas, o aún en series de oficinas dependiendo de la distribución física.

Definición de las Áreas Seguras

Las áreas seguras dentro de una oficina incluirán lugares como un centro de datos, el departamento de investigación y desarrollo, un laboratorio, un cuarto de cableado telefónico, un cuarto con sistema de red o cualquier otra área que requiera de controles adicionales de seguridad, no únicamente para restringir a los atacantes externos, sino también para limitar el acceso de los empleados internos. Las tecnologías de seguridad para un área incluyen lo siguiente:

- Lectores de tarjetas
- Teclados numéricos
- Tecnologías biométricas (p.ej., escáneres de huellas digitales, escáneres de retina, sistemas de reconocimiento de voz, etc.).
- Puertas de seguridad
- Escáneres de rayos X
- Detectores de Metales
- Cámaras
- Sistemas de detección de intrusos (rayo de luz, luz infrarroja, microondas, y/o ultrasónico)

Tome Nota

Las oficinas más pequeñas, que no están ocupadas durante la noche, pueden aprovechar los sistemas de monitoreo remoto y detección de intrusos en su perímetro interno. Las instalaciones más grandes generalmente tienen alguna actividad que ocurre durante la noche y los fines de semana, lo que hace que el uso de estas tecnologías sea más complicado.

Procesos de Seguridad del Sitio

Aún cuando la tecnología es un componente importante de la seguridad física de una empresa, los procesos que se ponen en marcha para apoyar esta tecnología, son igual de críticos. En realidad, debe tener estos procesos en todos los niveles de su sitio.

*** Tome Nota**

Hay cámaras disponibles en casi todos los teléfonos celulares que se encuentran actualmente en el mercado. Si necesita asegurar que esas cámaras no sean utilizadas en sus instalaciones, organice un plan para que se recojan los teléfonos en la puerta o para deshabilitar la función de cámara

En el perímetro externo, puede contar con un proceso para administrar la entrada al estacionamiento a través de una reja, o puede existir un proceso de qué tan a menudo las patrullas de vigilancia cuidan el estacionamiento. Se debe incluir en estos procesos la manera en que se documentarán los hallazgos, se vigilarán las entradas y las salidas y se responderá a los incidentes. Por ejemplo, el proceso de la ronda de vigilancia debe incluir instrucciones acerca de cómo hacerse cargo de un automóvil que no se encuentra cerrado o de una persona sospechosa, o con la mayor concientización, de posibles ataques terroristas o cómo manejar un paquete abandonado.

En el perímetro interno, puede contar con procesos que incluyan procedimientos para recabar la firma de visitantes, para la remoción de equipo, rotación de la vigilancia o para cuando la puerta principal no es cerrada con llave. Probablemente también debe contar con procesos para administrar las entregas, de cómo o cuando escoltar a visitantes dentro de las instalaciones, y aún acerca de qué tipo de equipo puede ser introducido al edificio. Por ejemplo, muchas empresas prohíben la introducción de equipo personal a la oficina, debido al riesgo de que un empleado pudiera utilizar su computadora personal para robar información valiosa de la compañía.

Una vez que ha alcanzado la capa de área segura, generalmente contará con procedimientos para controlar a quién le está permitido entrar al centro de datos y de qué forma tendrán acceso a él. Adicionalmente, contará con una variedad de mecanismos para asegurar que se otorgue el acceso únicamente a las personas autorizadas, incluyendo cuartos cerrados con llave, dispositivos biométricos, cámaras y vigilantes de seguridad.

▶ *Seguridad Informática*

La seguridad informática consiste en los procesos, procedimientos, políticas y tecnología utilizados para proteger el sistema de informática. Para los fines de este capítulo, la seguridad informática se referirá únicamente a la protección física de las computadoras; veremos otras facetas de la seguridad informática a lo largo del resto de este libro.

Además de las diversas medidas de seguridad física que ya hemos descrito, existen algunas herramientas adicionales que pueden ser utilizadas para proteger las computadoras en uso. Sin embargo, antes de hablar acerca de estas herramientas, primero tenemos que diferenciar entre los tres principales tipos de computadoras:

- **Servidores:** Estos son computadoras utilizadas para hacer funcionar las aplicaciones centralizadas y para entregar esas aplicaciones a través de una red. Ésta puede ser una red interna (como la red de un negocio) o incluso el Internet (para acceso público). La computadora que aloja su sitio web favorito es un excelente ejemplo de un servidor. Los servidores generalmente están configurados con capacidades

redundantes, que van desde discos duros hasta servidores con la completa inclusión de clústeres.

- **Computadoras de escritorio**: Estas computadoras generalmente se encuentran en entornos de oficina, escuelas y hogares. El objetivo de estas computadoras es ser utilizadas en un solo sitio y correr aplicaciones tales como el procesamiento de palabras, hojas de cálculo, juegos y otros programas locales. También pueden ser utilizadas para interactuar con aplicaciones centralizadas o para navegar por sitios web.
- **Computadoras móviles**: Esta categoría incluye laptops, *notebooks, tablets y netbooks.* Estas máquinas son utilizada para los mismos tipos de funciones que una computadora de escritorio, pero han sido creadas para ser utilizadas en múltiples ubicaciones (por ejemplo en el hogar y en la oficina). Debido a su tamaño más pequeño, las computadoras móviles alguna vez fueron menos potentes que las computadoras de escritorio, pero gracias a los avances en las tecnologías de micro procesamiento y almacenamiento, esta brecha se está reduciendo rápidamente.

Cada tipo de computadora (servidor, de escritorio y móvil) requiere de diferentes consideraciones de seguridad física. Por ejemplo, al asegurar un servidor, lo primero que se debe tomar en consideración es el lugar en donde estará ubicado. Generalmente, los servidores son mucho más caros que las computadoras de escritorio o las computadoras móviles y son utilizados para correr aplicaciones críticas, por lo que los tipos de seguridad que son utilizados generalmente en los servidores están basados en gran parte en su ubicación. Los servidores deben ser asegurados en centros de datos o cuartos de computadoras, en donde se puede tener la ventaja de un cuarto cerrado con llave, cámaras, y varias otras características de seguridad que han sido descritas en la lección anterior.

Si no tiene la capacidad para colocar a un servidor en un centro de datos o en un cuarto de computadoras, debe utilizar una de las siguientes tecnologías:

- **Cable de seguridad para la computadora:** Es un cable que está conectado de la computadora a un mueble o a la pared.
- **Gabinete / Rack de seguridad para la computadora:** Es un contenedor de almacenamiento que está asegurado por una puerta que se cierra con llave.

Las computadoras de escritorio generalmente están aseguradas con el mismo tipo de cables de seguridad para la computadora que se puede utilizar para los servidores. Las computadoras muchas veces son utilizadas en entornos de oficina seguros o en los hogares de las personas y no son especialmente costosas en comparación con otras tecnologías. Por lo tanto, la mayoría de las empresas no toman medidas extraordinarias para proteger a las computadoras de escritorio que se encuentran en sus oficinas.

Las computadoras portátiles, a diferencia de los servidores y las computadoras de escritorio, son altamente móviles, por lo que hay un conjunto de tecnologías únicas y más prácticas para proteger a estas máquinas de robo o daño. Algunos de estos métodos se describen en la siguiente sección.

Entender la Seguridad de los Dispositivos Portátiles

Los dispositivos portátiles constituyen uno de los mayores retos a los que se enfrentan en la actualidad los profesionales de la seguridad. Los dispositivos portátiles tales como laptops, PDAs (asistentes digitales personales), los teléfonos inteligentes, son utilizados para procesar información, enviar y recibir correo electrónico, almacenar enormes cantidades de datos, navegar por el Internet, e interactuar de manera remota con redes y sistemas internos. Cuando tomamos en consideración que se puede colocar una tarjeta de memoria MicroSD de 32 GB (ver la Figura 1-2) en un teléfono inteligente que un vicepresidente

ejecutivo puede utilizar para almacenar toda la información de investigación y desarrollo de la empresa, el potencial impacto para la compañía en caso que alguien llegase a robar ese teléfono es inimaginable. Como resultado de esto, la industria ofrece una cantidad de tecnologías para asegurar físicamente los dispositivos portátiles, incluyendo las siguientes:

★ Tome Nota

La seguridad de una base docking únicamente funciona si la activa y se asegura que esté fija a un objeto que no puede moverse. Muchas veces es igual de sencillo robar una laptop y su base docking como lo es robar únicamente la laptop

- **Base Docking:** Casi todas las estaciones de acoplamiento para computadoras portátiles están equipadas con características de seguridad. Estas pueden involucrar una llave, un candado, o ambos, dependiendo del proveedor y del modelo.
- **Cables de seguridad para laptop:** Utilizados junto con la USS (Ranura Universal de Seguridad), estos cables se conectan a la laptop y pueden ser enrollados alrededor de un objeto fijo como por ejemplo un mueble.
- **Cajas fuertes para laptop:** Estas son cajas fuertes de acero diseñadas especialmente para guardar una laptop y ser fijadas a una pared o a un mueble.
- **Software para la recuperación de robos:** Estas aplicaciones permiten rastrear a una computadora robada para que pueda ser recuperada.
- **Alarma para laptop:** Estas son alarmas sensibles al movimiento que suenan en caso que una laptop sea movida. Algunas también están diseñadas conjuntamente con sistemas de cables de seguridad de manera que suenen cada vez que se corte el cable.

Los PDAs y los teléfonos inteligentes generalmente son más difíciles de asegurar que una laptop; puesto que constituyen una tecnología nueva que hace muy poco saltó a la popularidad, únicamente están disponibles algunas herramientas de seguridad limitadas. Por el momento, se pueden configurar contraseñas para proteger a estos dispositivos, habilitar el cifrado y borrar remotamente los teléfonos que son administrados por una empresa. Algunos teléfonos inteligentes y PDAs también incluyen componentes de posicionamiento global que permiten rastrear su ubicación.

Por supuesto, existen mejores prácticas (y sí, éstas se basan en el sentido común) que pueden ser implantadas al asegurar tanto las laptop como los PDAs o los teléfonos inteligentes, incluyendo las siguientes:

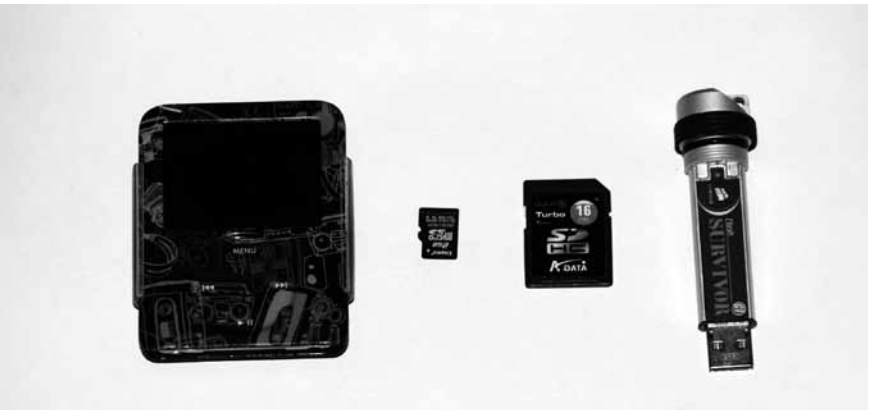
- **Mantenga su equipo siempre a la vista:** Debe mantener los dispositivos portátiles a su lado siempre que sea posible. Esto significa que al estar de viaje debe conservar sus dispositivos portátiles en su equipaje de mano. De la misma manera, conserve sus dispositivos portátiles a la vista cuando pase por los puntos de control en un aeropuerto.
- **Utilice la cajuela del automóvil:** Si viaja en automóvil y no puede llevar su dispositivo portátil a donde vaya cuando baje del automóvil, guárdelo en la cajuela cuando se estacione. No deje un dispositivo portátil a la vista en un vehículo que se queda solo, aunque sea por poco tiempo, y nunca lo deje en un vehículo durante toda la noche.
- **Utilice la caja fuerte**: Si se hospeda en un hotel, guarde su dispositivo portátil en una caja fuerte si esta se encuentra disponible.

Dispositivos y Discos Extraíbles

Además de los dispositivos portátiles, otra tecnología que presenta retos únicos para los profesionales de la seguridad son los dispositivos y discos extraíbles. Se pueden ver algunos ejemplos de dispositivos extraíbles comunes en la Figura 1-2.

Figura 1-2

Dispositivos extraíbles



Un ***dispositivo o disco extraíble*** es un dispositivo de almacenamiento que ha sido diseñado para ser sacado de una computadora sin apagarla. Estos dispositivos varían desde la tarjeta de memoria MicroSD, que tiene el tamaño de la uña de un dedo y puede almacenar hasta 32 GB de información, hasta un disco externo, el cual puede almacenar hasta 2 terabytes de información. Los floppy disks, CDs y DVDs también son considerados como unidades extraíbles, ya que pueden ser utilizados para almacenar información crítica.

Los dispositivos extraíbles generalmente se conectan a una computadora mediante puertos de comunicación externos como USB o Firewire, o en el caso de tarjetas de memoria, mediante lectores basados en USB. Estos dispositivos son utilizados para una variedad de propósitos, incluyendo el respaldo de información crítica, proporcionar almacenamiento adicional, transferir información entre computadoras y, algunas veces, hasta para correr aplicaciones. Esta forma de almacenamiento también es utilizada en reproductores de música como los iPods y Zunes, así como en reproductores personales de medios tales como los dispositivos Archos y Creative's Zen.

Existen tres tipos básicos de problemas de seguridad relacionados con el almacenamiento extraíble:

- Pérdida
- Robo
- Espionaje

La pérdida de un dispositivo de almacenamiento es uno de los problemas de seguridad más comunes con los que nos podemos encontrar. Las unidades USB son particularmente problemáticas en este aspecto. Generalmente son del tamaño de un paquete de chicles o más pequeñas, por lo que estas unidades se olvidan con frecuencia en la sala de conferencias, en las habitaciones de hotel o en las bolsas de los asientos de un avión. El reto al cual se enfrenta es el de cómo asegurar los gigabytes de información que se pierden junto con estas unidades. Actualmente, estos dispositivos pueden ser protegidos mediante la autenticación como el encriptado. Asimismo, Windows 7, el Servidor Windows 2008 R2, y BitLocker to Go lanzado por Microsoft, pueden ser utilizados para proteger la información en dispositivos portátiles de almacenamiento. Adicionalmente, algunas empresas pueden ofrecer su propio mecanismo de protección, tal como IronKey. Por supuesto, es necesario recalcar a los usuarios el valor de la información, así como lo fácil que es perder los dispositivos portátiles de almacenamiento.

El robo es un problema al que se enfrenta cualquier equipo portátil. Muchas de las medidas para la prevención de robos, acerca de las cuales hemos hablado con relación a estos equipos, también se aplican a los dispositivos portátiles de almacenamiento. Por

ejemplo, conserve consigo las unidades siempre que le sea posible. Cuando no las pueda llevar, asegúrelas en la caja fuerte de un hotel, en un cajón cerrado con llave o en alguna otra ubicación segura. No deje un equipo portátil de información a la vista, donde puede ser removido con facilidad del área. Recuerde, aún cuando los dispositivos portátiles son relativamente baratos en sí mismos, la información que se encuentra almacenada en ellos puede ser irremplazable, o lo que es peor aún, confidencial.

Referencia Cruzada

Frecuentemente se utiliza la encriptación para asegurar la información que se encuentra en las unidades extraíbles. Este método es analizado detalladamente en la Lección 2

Por último el área en la cual estos dispositivos presentan un problema de seguridad está relacionada con el espionaje. Muchos dispositivos de almacenamiento vienen en presentaciones muy pequeñas, lo cual las hace sumamente adecuadas para el espionaje. Por ejemplo, se pueden adquirir unidades *flash* disfrazadas de plumas, relojes o como parte de una navaja. Para complicar aún más el problema, todos los dispositivos cotidianos tales como reproductores de música y teléfonos celulares muchas veces cuentan con múltiples gigabytes de almacenamiento. Aún cuando logre prohibir unidades externas y reproductores de música en sitios de trabajo, el quitar a los empleados los teléfonos celulares es virtualmente imposible. Entonces, ¿cómo puede proteger su entorno de este tipo de amenaza a la seguridad?

La clave para esta amenaza no es tratar de defender el entorno de los dispositivos portátiles, sino proteger la información frente a cualquier acceso no autorizado. Es aquí donde el principio de privilegio mínimo es crítico, si se asegura que los empleados únicamente puedan tener acceso a la información, sistemas y redes que necesitan para desempeñar su trabajo, puede hacer que la tarea de mantener la información crítica fuera de las unidades portátiles sea mucho más fácil.

Tome Nota

Algunos lugares de trabajo resuelven los problemas relacionados con los dispositivos de almacenamiento portátiles mediante el uso de configuraciones de hardware o software que prohíben su utilización. Aún cuando ésta puede ser una estrategia eficaz, también es costosa y requiere de la utilización de muchos recursos. Por lo tanto, es únicamente en un número limitado de negocios donde esta estrategia puede ser implementada con eficacia.

Keyloggers

Un ***keylogger*** es un dispositivo físico o lógico utilizado para registrar las pulsaciones en el teclado. Un atacante colocará, ya sea un dispositivo entre el teclado y la computadora, o instalará un programa de software para registrar cada pulsación en el teclado, por lo que a continuación él puede utilizar un software para reproducir y capturar la información tal como la ID y contraseñas del usuario, números de tarjeta de crédito, números de Seguro Social, e incluso correos electrónicos confidenciales y otra información. También existen sniffers inalámbricos de teclado que pueden interceptar las pulsaciones enviadas entre un teclado inalámbrico y una computadora.

Referencia Cruzada

La Lección 5 contiene información más detallada acerca del antimalware y las tecnologías de firewall en una estación de trabajo

Para proteger contra un keylogger físico, la mejor herramienta es una inspección ocular. Observe la conexión entre el teclado y la computadora. Si se encuentra presente un dispositivo extra entre ambos, alguien está tratando de capturar sus pulsaciones en el teclado. Esto es particularmente importante al estar trabajando en computadoras compartidas o computadoras públicas, donde los atacantes utilizan keyloggers para lanzar una amplia red y capturar cualquier información crítica que alguien pudiese introducir.

La mejor defensa contra un software keylogger es el uso de un software antimalware actualizado. Muchos keyloggers son identificados como malware por estas aplicaciones. También puede aprovechar el Control de Cuenta de Usuario y firewalls basados en el host para evitar que sea instalado un software keylogger.

Para defenderse en contra del sniffer de teclado inalámbrico, su mejor apuesta es asegurar que su teclado inalámbrico soporte conexiones encriptadas. La mayoría de los teclados inalámbricos actuales operan, ya sea en un modo encriptado por defecto o por lo menos le permitirá configurar la encriptación en el transcurso de la instalación.

Resumen de Capacidades

- Antes de comenzar a asegurar su entorno, necesita tener un entendimiento fundamental de los conceptos estándar de seguridad.
- CIA, las siglas que representan confidencialidad, integridad y disponibilidad, representa los objetivos básicos de un programa de seguridad de la información.
- La confidencialidad está relacionada con cómo mantener la información, las redes y los sistemas seguros frente a un acceso no autorizado.
- Uno de los objetivos de un programa de seguridad de información exitoso es asegurar la integridad, o que la información esté protegida en contra de cualquier cambio no autorizado o accidental.
- La disponibilidad es definida como la característica para que un recurso esté accesible para un usuario, aplicación o sistema de computación, siempre que sea requerido.
- La administración de amenazas y riesgos es el proceso mediante el cual se identifica, evalúa y da prioridad a las amenazas y los riesgos.
- Un riesgo es generalmente definido como la probabilidad de que un evento pueda ocurrir.
- Una vez que ha dado prioridad a sus riesgos, existen cuatro respuestas generalmente aceptadas para enfrentarlos: evitar, aceptar, mitigar y transferir.
- El principio de privilegio mínimo es una disciplina de seguridad que requiere que un usuario, sistema o aplicación no otorgue ningún privilegio adicional al que fuese necesario para desempeñar su función o trabajo.
- Una superficie de ataque consiste en un conjunto de métodos y vías que puede utilizar un atacante para entrar a un sistema y causar un daño potencial. Entre mayor sea la superficie de ataque, mayor será el riesgo de un ataque exitoso.
- La clave para frustrar un ataque de ingeniería social es la concientización de los empleados. Si sus empleados saben de lo que se deben cuidar, un atacante tendrá muy poco éxito.
- La seguridad física utiliza defensas a profundidad o un enfoque de seguridad por niveles que controla quién puede tener acceso físico a los recursos de una empresa.
- Las instalaciones físicas se pueden dividir en tres áreas lógicas: el perímetro externo, el perímetro interno y áreas seguras.
- La seguridad informática se compone de los procesos, procedimientos, políticas y tecnologías utilizadas para proteger los sistemas informáticos.
- Los dispositivos portátiles y el almacenamiento en dispositivos portátiles se encuentran entre los mayores riesgos a los que se enfrentan actualmente muchos profesionales de la seguridad debido a su tamaño y portabilidad.
- Un keylogger es un dispositivo físico o lógico utilizado para capturar pulsaciones del teclado.

» Evaluación de Conocimientos

Opción Múltiple

Encierre en un círculo la letra o letras que correspondan a la mejor respuesta o respuestas.

1. ¿Cuáles de las siguientes son respuestas válidas frente a un riesgo? (Elija todas las aplicables).
   a. Mitigar
   b. Transferir
   c. Invertir
   d. Evitar
2. ¿Cuáles de los siguientes son considerados como dispositivos o discos extraíbles? (Elija todos los aplicables).
   a. iPod
   b. Netbook
   c. USB flash drive
   d. Floppy drive
3. ¿Cuáles de las siguientes medidas serían consideradas como medidas de seguridad apropiadas para el perímetro exterior de seguridad de un edificio? (Elija todas las aplicables).
   a. Detector de movimiento
   b. Iluminación en el estacionamiento
   c. Torniquetes de control de acceso
   d. Guardias de seguridad
4. Está viajando por negocios y se dirige a una cena con un cliente. No puede llevar su laptop consigo al restaurant. ¿Qué es lo que debería hacer con el dispositivo? (Elija la mejor respuesta).
   a. Guardar la laptop en la cajuela de su automóvil.
   b. Guardar la laptop en un cajón de la cómoda donde no se vea.
   c. Fijar la laptop a un mueble mediante un cable de seguridad para laptop.
   d. Llevar la laptop a la recepción y pedir que la guarden ahí.
5. ¿El proceso de eliminación de un riesgo al optar por no participar en una acción o actividad describe a cuál de los siguientes?
   a. Mitigar
   b. Riesgo residual
   c. Evitar
   d. Aceptar
6. Acaba de ser ascendido a Director en Jefe de Seguridad en su empresa de fabricación de auto partes y está tratando de identificar tecnologías que ayudarán a garantizar la confidencialidad de sus técnicas exclusivas de fabricación. ¿Cuáles de las siguientes tecnologías podría utilizar para ayudarle en este esfuerzo? (Elija todas las aplicables).
   a. Encriptación fuerte
   b. Guardias de seguridad

c. Cajas fuertes para laptop
d. Autenticación fuerte

7. ¿Qué significan las siglas CIA?
   a. Confidencialidad, identidad, control de acceso
   b. Confidencialidad, integridad, control de acceso
   c. Confidencialidad, integridad, disponibilidad
   d. Control, identidad, control de acceso

8. Lo han puesto a cargo del departamento de seguridad corporativa y su jefe le ha pedido que le ayude a entender lo que significan los principios básicos de seguridad. ¿Cuál de estas explicaciones es la que debe dar a su jefe?
   a. Los principios básicos de seguridad se refieren al perímetro interno de seguridad al crear un entorno de capas de seguridad física.
   b. Los principios básicos de seguridad se refieren a los principios de confidencialidad, disponibilidad e integridad.
   c. Los principios básicos de seguridad se refieren a aprovechar las mejores prácticas de seguridad.
   d. Los principios básicos de seguridad se refieren a los cuatro métodos para enfrentar riesgos.

9. Como el Director en Jefe de Seguridad para una pequeña empresa de procesamiento de registros médicos, acaba de terminar de configurar la seguridad física para su nueva oficina. Por lo tanto se ha asegurado particularmente de que el estacionamiento se encuentre iluminado, que cuenta con vigilantes tanto en la puerta, como llevando a cabo rondas periódicas, y que cuenta con lectores de tarjetas en todo el edificio en los lugares clave. También ha colocado tecnología biométrica de acceso en la puerta del centro de datos. Adicionalmente, cuenta con cámaras en el estacionamiento, en las entradas al edificio y en las entradas al centro de datos. Este tipo de implementación se conoce cómo: (Elija la mejor respuesta).
   a. control de acceso
   b. principios básicos de seguridad
   c. mejores prácticas de seguridad
   d. defensa en profundidad

10. ¿Qué nombre le da al proceso de deshabilitar servicios y puertos innecesarios para hacer que su sistema sea más seguro?
    a. Reducir el **á**rea de la superficie de ataque
    b. Mitigar a un Troyano
    c. Evasión de seguridad
    d. Defensa a profundidad

Complete los espacios en blanco

1. _____es la característica de un recurso que garantiza que el acceso está restringido a únicamente los usuarios, las aplicaciones o los sistemas informáticos autorizados.

2. Si está implementando tecnologías para restringir el acceso a un recurso, está practicando el principio de seguridad conocido como _____.

3. La implementación de múltiples capas de seguridad se llama _____?

4. Una acción o acontecimiento que pudiese resultar en el incumplimiento, interrupción o corrupción de un sistema al explotar vulnerabilidades conocidas o desconocidas es un(a) _____.

5. Acaba de aceptar un nuevo trabajo como Gerente de Riesgos de una empresa farmacéutica de tamaño mediano y su primera tarea es llevar a cabo una evaluación formal de riesgos. Muy probablemente va a registrar los resultados de su evaluación de riesgos en un(a) _____.

6. Una secretaria en su oficina acaba de colgar una llamada de una persona quien dijo que estaba llamando del departamento corporativo de TI. La persona que llamó hizo una serie de preguntas acerca de la configuración del equipo de la secretaria, y solicitó que le dijera cual era su nombre de usuario y contraseña. En esta situación, la secretaria muy probablemente fue una víctima de _____.

7. La consistencia, precisión y validez de los datos o la información se llama _____.

8. Está viajando por negocios y decide utilizar una computadora en el centro de negocios del hotel para revisar su correo electrónico y pagar varias cuentas. Cuando se sienta frente a la computadora, se da cuenta que hay un conector extra entre el teclado y la computadora. Lo más probable es que se ha encontrado con un(a)_____.

9. Considere que es el Gerente de Riesgos de un banco regional, y acaba de implementar un nuevo sistema de lector de tarjetas para hacer frente a un riesgo de control de acceso. Aún cuando su solución ha mitigado el peligro, todavía queda un pequeño riesgo remanente relacionado con el control de acceso. A este riesgo se le conoce como el (la) _____.

10. Cuanto mayor sea el (la) _____ de un entorno en particular, mayor será el riesgo de un ataque exitoso.

Listo para el Lugar de Trabajo

→ Entendiendo lo Básico

Entender los conceptos de seguridad constituye únicamente el primer paso para aprender acerca de la seguridad. Como administrador de red u oficial de seguridad, se sorprenderá de cuánto le ayudará el tomar en cuenta estos principios básicos a la hora de planear, implementar y actualizar el programa general de seguridad de su empresa.

» Evaluación de Competencia

Escenario 1-1: Diseño de una Solución de Seguridad Física

Considere que es el Gerente de Seguridad de un banco de tamaño mediano. Le han pedido que diseñe una solución de seguridad para mantener a los intrusos fuera después de las horas de trabajo. Las tres áreas del banco que debe asegurar son el estacionamiento, el perímetro del edificio y la bóveda de seguridad. Prepare una lista de las tecnologías que utilizará en cada una de estas áreas.

Escenario 1-2: Asegurar un Dispositivo Portátil

Considere que es el Gerente de IT de una empresa de servicios jurídicos con 5,000 empleados. Está en el proceso de introducción de nuevos dispositivos portátiles para su departamento de ventas. ¿Qué procesos y tecnologías utilizará para conservar a estos dispositivos físicamente seguros?

» Evaluación de Habilidad

Escenario 1-3: Analizando la Confidencialidad, Integridad, y Disponibilidad

Dentro de su empresa, tiene un servidor llamado Servidor 1, el cual ejecuta el Servidor Windows 2008 R2. En el Servidor 1, crea y comparte una carpeta llamada Datos en el drive C. Dentro de la carpeta de Datos, crea una carpeta para cada usuario dentro de su empresa. A continuación coloca el cheque de pago electrónico del salario de cada persona en su carpeta. Más tarde se entera que Juan pudo entrar y cambiar algunos de los cheques electrónicos y borrar otros. Explique cuál de los componentes CIA no fue cumplido en este escenario.

Escenario 1-4: Examinando la Ingeniería Social

Considere que trabaja para Contoso Corporation. Su director quiere que arme un curso de capacitación acerca de la seguridad del usuario final. Para comenzar, utilice el Internet para investigar tres casos o instancias en las cuales las personas utilizaron la ingeniería social para irrumpir en un sistema y prepare una lista de cómo intentaron obtener acceso.

Lección 2

Autenticación, Autorización y Auditoría

Matriz del Dominio Objetivo

Habilidades/Conceptos	Descripción del Objetivo Principal	Número de Dominio Objetivo
Seguridad al iniciar con autenticación	Entendiendo la función de autenticación de un usuario.	2.1
Comparación de derechos y permisos	Entendiendo los permisos.	2.2
Uso de la función de auditoría para completar el cuadro de seguridad	Entendiendo las directivas de auditoría.	2.4
Uso de encriptación para proteger los datos	Entendiendo la encriptación.	2.5

Términos clave

- Lista de control de acceso (ACL)
- Directorio activo (Active Directory)
- Administración compartida
- Encriptación asimétrica
- Autenticación
- Autorización
- Cuentas de usuario
- Biométrica
- Auditoría
- *BitLocker To Go* [función de encriptación]
- Ataque por fuerza bruta [ataque intensivo para descifrar códigos de seguridad]
- Grupos predefinidos
- Cadena de certificados (Certificate Chain)
- Lista de certificados revocados (CRL)
- Cuenta de equipo
- Desencriptación
- Ataque por diccionario
- Certificado digital
- Firma digital
- Controlador de dominio
- Usuario de dominio
- Permisos efectivos
- Encriptación
- Permisos explícitos
- Grupo
- Función hash
- Permisos heredados
- Seguridad del protocolo Internet (IPsec)
- Kerberos
- Clave
- Cuenta de usuario local
- Servidor miembro
- Autenticación de multifactor
- Reconocimiento de firma
- NTFS [Sistema de Archivos NT]
- Permisos NTFS
- NTLM [administrador LAN NT]
- Unidades organizacionales (OU)
- Propietario
- Contraseña
- Permiso
- Número de identificación personal (PIN)
- Infraestructura de llave pública (PKI)
- Registro
- Derecho
- Protocolo de Capa de Conexión Segura (SSL)
- Administrador de cuentas de seguridad (SAM)
- Token de seguridad [dispositivo electrónico para facilitar la autenticación]
- Permisos compartidos
- Carpeta compartida
- Inicio de sesión (SSO)
- Tarjeta inteligente
- Encriptación simétrica
- Syslog
- Cuenta de usuario
- Red privada virtual (VPN)

El DTI [Director de Tecnología Informática] de su empresa lo involucra en la discusión sobre temas de seguridad. Durante la conversación, le pregunta qué medidas ha implementado la empresa para asegurar que los usuarios puedan acceder sólo a lo que se requiere y nada más. Usted le responde explicando que ha construido su modelo de seguridad de la organización usando las tres "A": Autenticación, Autorización y Auditoría. Desafortunadamente, él quiere saber más acerca de su modelo, ¿cómo le respondería?

▪ Seguridad al iniciar con Autenticación

↓ EN RESUMEN

En el ámbito de la seguridad de la información, AAA (Autenticación, Autorización y Auditoría) es un modelo líder para el control de acceso. En él, la ***Autenticación*** es el proceso de identificación de individuo, usualmente basado en un nombre de usuario y una contraseña. Después de que un usuario es autenticado, él o ella pueden acceder a los recursos de red con base en su autorización. La ***Autorización*** es el proceso de dar a los individuos acceso a los objetos del sistema basándose en su identidad. Finalmente, las ***cuentas de usuario***, también ***Auditoría*** es el proceso de mantener un registro de la actividad de un usuario mientras se encuentra usando los recursos de red, incluyendo la cantidad de tiempo en red, los servicios a los que accede mientras tanto y la cantidad de datos transferidos durante cada sesión.

La función de ***r***econocimiento de firma (nonrepudiation) impide que una de las partes rechace las acciones que ha llevado a cabo. Si ha establecido una adecuada autenticación, autorización y auditoría, entonces tendrán lugar mecanismos apropiados de ***r***econocimiento de firma y ningún usuario podrá rechazar las acciones que él o ella ha llevado a cabo mientras trabaja en el sistema de su organización.

☑ Listo para la Certificación

¿Puede citar las diferentes formas de autenticación? --2.1

Antes de que los usuarios puedan acceder a un equipo o un recurso de red, es muy probable que tengan que registrarse para probar que se trata de quienes dicen ser y verificar si cuentan con los derechos y permisos requeridos para acceder a los recursos de red.

El registro de usuario es el proceso a través del cual una persona es reconocida por el sistema de un equipo o red de forma tal que pueda iniciar una sesión. Un usuario puede ser autenticado a través de uno o más de los siguientes métodos:

- **Mediante algo que se sabe**: por ejemplo, mediante el suministro de una contraseña o número de identificación personal (PIN).
- **Mediante algo que se posee**: por ejemplo, proporcionando un pasaporte, tarjeta inteligente o tarjeta de identificación.
- **Demostrando quién se es**: por ejemplo, por factores biométricos de ingreso basados en huellas digitales, escaneo de retina, reconocimiento de voz, etc.

Cuando dos o más métodos de autenticación se usan para autenticar a alguien, se dice que se trata de un sistema de ***autenticación de multifactor***. Desde luego, un sistema que usa dos métodos de autenticación (tales como una tarjeta inteligente y contraseña) podemos decir que se trata de un sistema de autenticación de dos factores.

▶ *Autenticación mediante algo que se sabe*

Tanto para equipos de cómputo individuales como para redes enteras, el método más común de autenticación es la contraseña. Una ***contraseña*** es una serie secreta de caracteres que habilita a un usuario a tener acceso a un archivo específico, equipo de cómputo o programa.

Contraseñas

Cuando se quiere acceder a un archivo, equipo de cómputo o red, los *hackers* [piratas informáticos] intentarán primero violar las contraseñas tratando con posibilidades obvias, incluyendo los nombres y cumpleaños de la esposa o hijos del usuario, términos clave utilizadas por el usuario o los pasatiempos del usuario. Si estos intentos no funcionan, la mayoría de los *hackers* tratarán entonces con un ***Ataque por fuerza bruta***, que consiste en intentar todas las posibles combinaciones de caracteres como el tiempo y el dinero les permitan. Una variante del ataque por fuerza bruta es el ***ataque por diccionario***,

que intenta todas las palabras en uno o más diccionarios. También intentan con listas de contraseñas comunes.

Para construir una contraseña más segura, tiene que escoger una palabra que nadie pueda adivinar. De tal forma, debe tratarse de una cadena suficientemente larga y debe considerarse una contraseña fuerte y compleja. Para mayor información sobre cómo crear contraseñas fuertes, visite los siguientes sitios web:

http://www.microsoft.com/protect/fraud/passwords/create.aspx

https://www.microsoft.com/protect/fraud/passwords/checker.aspx?WT.mc_id=Site_Link

Debido a que los equipos de cómputo actuales son mucho más potentes que los equipos de cómputo del pasado (que se usan con frecuencia para violar contraseñas), algunas personas recomiendan usar contraseñas de al menos 14 caracteres de largo. Sin embargo, recordar contraseñas largas puede ser incómodo para algunas personas, y estos individuos probablemente escribirán las contraseñas en pedacitos de papel cerca de su escritorio. En estos casos, deberá empezar a buscar otras formas de autenticación, tales como una tarjeta inteligente o por medio de la biométrica.

Los usuarios podrían también cambiar sus contraseñas de forma regular; así, si la contraseña de un usuario es revelada a alguien más, esto durará solamente hasta que la contraseña ya no sea válida. Además, el cambio de contraseñas de forma rutinaria también acorta la cantidad de tiempo que un individuo tiene para adivinar su contraseña, porque él o ella tendrán que volver a empezar nuevamente todo el proceso de violación de la clave una vez que la contraseña haya sido cambiada.

Microsoft incluye la configuración de directivas de contraseñas dentro de las directivas de grupos de forma que fácilmente se pueden seguir los estándares como el número mínimo de caracteres, el nivel mínimo de complejidad de la contraseña así como la frecuencia recomendable para que los usuarios las cambien, la periodicidad con la que los usuarios podrán usarlas de nuevo, entre otras opciones.

Aunque las contraseñas son el método de seguridad más fácil de implementar y el método más popular de autenticación, su uso también tiene importantes inconvenientes, incluyendo la probabilidad de que sean robadas, burladas y/u olvidadas. Por ejemplo, un *hacker* puede llamar al departamento de TI en busca de soporte y pretender ser un usuario legítimo, eventualmente puede convencer al departamento de restablecer la contraseña de un usuario para los que sea que él o ella requiera tal información.

Con tales escenarios, es esencial que se establezca un proceso de seguridad para restablecer todas las contraseñas del usuario. Por ejemplo, se puede establecer un proceso de autoservicio en el que la identidad de un usuario es verificada por medio de preguntas y comparando las respuestas con las que han sido registradas anteriormente, tales como la fecha de cumpleaños de la persona, el nombre de su película favorita, el nombre de su mascota, etc. Sin embargo, esto puede ser adivinado con cierta facilidad por parte de un atacante informático, determinado a partir de una búsqueda sencilla o descubierto a través de ingeniería social.

Por lo tanto, al restablecer contraseñas, se debe contar con un método para identificar de manera positiva al usuario que solicita el cambio. También debe evitarse el envío de contraseñas nuevas vía correo electrónico porque, el hacker probablemente también tendrá acceso a la cuenta de correo electrónico del usuario y podrá obtenerla también. Para evitar estos problemas, puede comunicarse frente a frente con la persona que solicita el cambio de contraseña y pedir su identificación. Desafortunadamente, con redes muy grandes y redes que incluyen muchos lugares físicos, esto podría no ser viable. También se puede regresar

la llamada y dejar la contraseña en el correo de voz de la persona al cual él o ella tendrá que acceder proporcionando un PIN, o se puede enviar la contraseña al gerente del usuario o al auxiliar administrativo. En cualquier caso, se debe asegurar que el usuario cambie la contraseña inmediatamente después de que él o ella ingresen.

Número de Identificación Personal (PIN)

Un ***número de identificación personal (PIN)*** es una contraseña numérica secreta compartida entre un usuario y un sistema que puede ser usado para autenticar al usuario en el sistema. Debido a que estos consisten solamente de dígitos y son relativamente cortos (usualmente cuatro dígitos), los PIN son usados sólo en casos de baja seguridad, tales como obtener acceso a un sistema, o en combinación con otros métodos de autenticación.

▶ *Autenticación por medio de algo que se posee*

Una segunda categoría de autenticación es con base en algo que se posee. Los ejemplos más comunes de este tipo de autenticación involucra el uso de certificados digitales, tarjetas inteligentes y tokens de seguridad.

Un ***certificado digital*** es un documento electrónico que contiene una identidad, tal como un nombre de usuario o de organización, junto con una clave pública correspondiente. Debido a que un certificado digital es usado para probar la identidad de una persona, puede también ser usado para el proceso de autenticación. Se puede comparar al certificado digital con una licencia de conducir o pasaporte que contiene su fotografía y su huella digital de forma que no hay duda de quién es el usuario.

Una ***tarjeta inteligente*** es una tarjeta de bolsillo con circuitos integrados incorporados que consta de componentes de almacenamiento de memoria no volátiles y una lógica de seguridad posiblemente dedicada. La memoria no volátil es memoria que no olvida su contenido al apagar el equipo. Este tipo de memoria puede contener certificados digitales para probar la identidad de la persona que porta la tarjeta, y puede también contener información de los permisos y del acceso. Debido a que las tarjetas inteligentes pueden ser robadas, algunas no tienen ninguna marca sobre ellas; esto hace difícil a un ladrón identificar a qué da acceso la tarjeta. Además, muchas organizaciones solicitan a los usuarios proporcionar contraseñas o PIN en combinación con sus tarjetas inteligentes.

Un ***token de seguridad*** (o algunas veces dispositivo token, hard token, token de autenticación, token USB, token de encriptación) es un dispositivo físico proporcionado a un usuario autorizado de un equipo de cómputo para facilitar su autenticación. Los aparatos tokens son generalmente lo suficientemente pequeños para ser llevados en el bolsillo y con frecuencia están diseñados para ir unidos a un "llavero" que porta el usuario. Algunas de estos token de seguridad incluyen un conector tipo USB, funciones RFID o interfaz inalámbrica Bluetooth para facilitar la transferencia de una secuencia de números clave generada para un sistema cliente. Algunos token de seguridad pueden también incluir tecnología adicional, tal como una contraseña estática o certificado digital incorporado en el token de seguridad, de manera muy similar a una tarjeta inteligente. Otros token de seguridad pueden automáticamente generar un segundo código que los usuarios deben ingresar para poder ser autenticados.

Autenticación demostrando quién se es

La Biometría es un método de autenticación que identifica y reconoce personas con base en rasgos físicos, tales como huellas dactilares, reconocimiento de rostro, reconocimiento de iris, escaneo de retina y reconocimiento de voz. Muchos equipos de cómputo portátiles incluyen un escáner dactilar, y es relativamente fácil instalar dispositivos biométricos sobre las puertas y gabinetes para verificar que sólo personas autorizadas entren a áreas de seguridad.

Para usar dispositivos biométricos (ver Figura 2-1), se debe contar con un lector biométrico o dispositivo de escaneo, programas que conviertan la información escaneada en digital y compare puntos de coincidencia, y una base de datos que almacene los datos biométricos a comparar.

Figura 2-1

Escáner dactilar

Para iniciar el sistema biométrico, se necesitará configurar una estación en la que un administrador inscriba a cada usuario; esto incluye el escaneo de la característica biométrica que quiere usar para el proceso de autenticación. Cuando se selecciona un método biométrico, se debe considerar su desempeño, dificultad, confiabilidad, aceptación y costo. También se necesita tomar en cuenta las siguientes características:

- Índice de falsos rechazos **(falsos negativos)**: Este es el porcentaje de usuarios autorizados a quienes se les negó el acceso indebidamente.
- Índice de aceptaciones falsas **(falsos positivos)**: Este es el porcentaje de usuarios no autorizados a quienes se permitió el acceso indebidamente.

Introducción a RADIUS y TACACS+

Cuando compra un nuevo equipo de cómputo y crea una cuenta de usuario local e ingresa, está siendo autenticado con el nombre de usuario y contraseña. Para las corporaciones, los equipos de cómputo pueden ser parte de un dominio, cuya autenticación puede ser proporcionada por el controlador de dominios. En otros casos, necesita proporcionar la autenticación, autorización y auditoria de manera centralizada, cuando los usuarios necesitan conectarse a un servicio de red. Los dos protocolos usados comúnmente que proporcionan estas funciones son el de RADIUS (Siglas en inglés para "autenticación y autorización para aplicaciones de acceso a la red o movilidad IP") y TACACS+ (siglas en inglés para "sistema de control de acceso del controlador de acceso a terminales")

Un servidor RADIUS o TACACS+ reside en un sistema remoto y responde a consultas de los clientes tales como Clientes de VPN [red privada virtual], puntos de acceso inalámbrico, routers y switches. El servidor autentica después combinaciones de nombre de usuario/contraseñas (autenticación), determina si los usuarios tienen permitido conectarse al cliente (autorización), y establece la conexión (registro de acciones).

RADIUS es un mecanismo que permite la autenticación vía conexión de internet y otras conexiones de red, incluyendo marcaje por módem, puntos de acceso inalámbrico, servidores de VPN y web. Como es un estándar IETF, ha sido implementado por la mayoría de los principales fabricantes de sistemas operativos, incluyendo Microsoft. Por ejemplo, en Windows Server 2008, Network Policy Server (NPS) puede ser usado como un servidor RADIUS para realizar la autenticación, autorización y registro de acciones para los clientes RADIUS. Puede ser configurado para usar un dominio de Servidor Microsoft Windows NT 4.0, un dominio Servicios de Dominio con Active Directory (AD DS), o base de datos de cuentas de usuarios de un Administrador de Cuentas de Seguridad local (SAM) para autenticar las credenciales del usuario para los intentos de conexión. NPS usa las propiedades de conexión de internet de la cuenta de usuario y de las directivas de red para autorizar una conexión.

Otro servidor AAA centralizado competente es el TACACS+, el cual fue desarrollado por Cisco. Cuando diseñó el TACACS+, Cisco incorporó gran parte de la funcionalidad existente de RADIUS y la extendió para cumplir sus necesidades. Desde un punto de vista de las características, TACACS+ puede ser considerado una extensión del RADIUS.

▶ *Ejecutar Como*

Debido a que los administradores tienen acceso total a equipos de cómputo individuales o redes enteras, se recomienda que use una cuenta de usuario estándar que no sea de administrador para realizar la mayoría de las tareas. Luego, cuando necesite realizar tareas administrativas, puedes usar el comando Ejecutar como o las opciones incorporadas que están incluidas en los sistemas operativos de Windows.

En las versiones previas de Windows, tenía que usar una cuenta de administrador para hacer ciertas cosas, tales como cambiar la configuración del sistema o instalar programas. Si se conectaba como usuario con permisos limitados, el comando Ejecutar eliminaba la necesidad de cerrar la sesión y volverla a iniciar como administrador.

En las versiones más recientes de Windows, incluyendo Windows 7 y Windows Server 2008 R2, el comando Ejecutar ha sido modificado a Ejecutar como administrador. Con Control de Cuenta de Usuario (UAC), rara vez tendrá que usar el comando Ejecutar como administrador, debido a que Windows automáticamente solicita una contraseña de administrador cuando se necesita. El UAC se discute a detalle en la Lección 5.

→ Ejecutar un programa como administrador

PREPÁRESE. Para ejecutar un programa como administrador, realice los siguientes pasos:

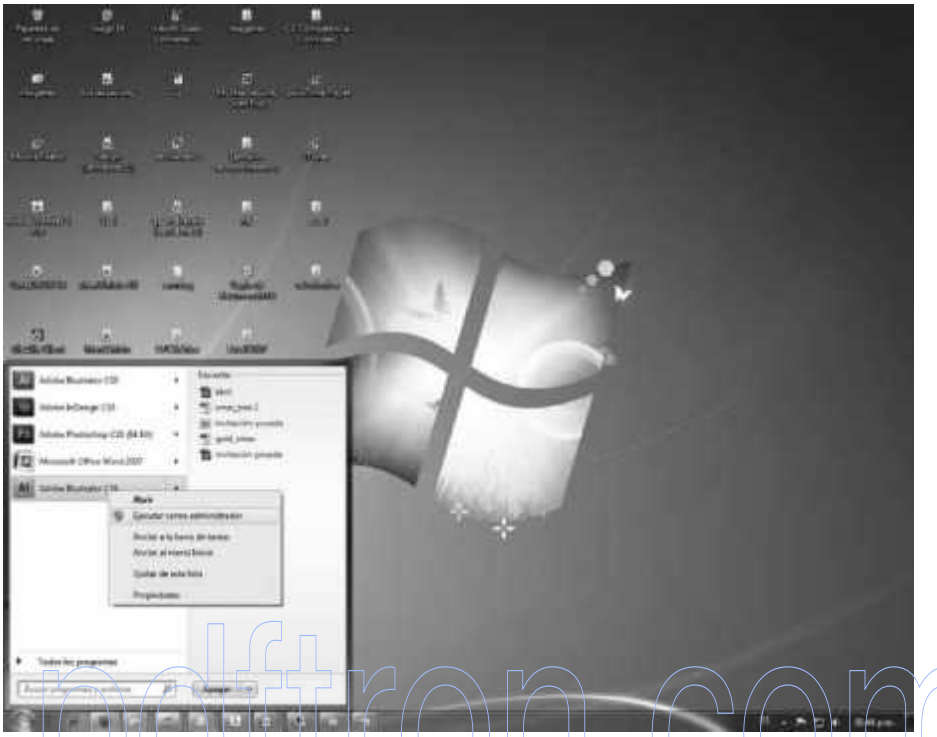
1. Haga clic derecho en el icono del programa o archivo que desea abrir, y luego en Ejecutar como administrador. Ver Figura 2-2.
2. Seleccione la cuenta de administrador que quiere usar, escriba la contraseña y luego haga clic en Sí.

Puede también usar el comando runas.exe. Por ejemplo, para ejecutar widget.exe como un administrador, deberá ingresar el siguiente comando:

- `runas /user:admin /widget.exe`

Figura 2-2

Uso de la opción Ejecutar como administrador



Introducción a los Servicios de directorio utilizando Directorio activo (Active Directory)

EN RESUMEN

Un servicio de directorio almacena, organiza y proporciona acceso a información en un directorio. Se utiliza para localizar, manejar y administrar elementos comunes y recursos de red, tales como volúmenes, carpetas, archivos, impresoras, usuarios, grupos, dispositivos, números telefónicos, etc. Un servicio de directorio popular usado por muchas organizaciones es el Directorio activo de Microsoft.

Directorio activo (Active Directory) es una tecnología creada por Microsoft que proporciona una variedad de servicios de red, incluyendo lo siguiente:

- Protocolo Ligero de Acceso a Directorios (LDAP)
- Autenticación basada en Kerberos e Inicio de sesión único (SSO)
- Asignación de nombres con base en DNS y otra información de red
- Ubicación central para administración de red y delegación de autoridad

El Protocolo Ligero de Acceso a Directorios (LDAP), es un protocolo de aplicación para consulta y modificación de servicios de directorio que usa datos que se ejecutan en TCP/IP. Dentro del directorio, la serie de objetos es organizada de manera lógica jerárquica de forma que se pueden encontrar y manejar fácilmente. La estructura puede reflejar los límites geográficos u organizacionales, aunque tiende a usar nombres DNS para estructurar

los niveles superiores de la jerarquía. En un lugar más profundo del directorio, puede haber entradas que representan personas, unidades organizacionales, impresoras, documentos, grupos de personas o cualquier otra cosa que simbolice una entrada de árbol (o múltiples entradas). El LDAP usa el puerto 389 de TCP.

Kerberos es el protocolo predeterminado de autenticación en red del equipo de cómputo, que permite a los host probar su identidad en una red no segura de una manera segura. También puede proporcionar autenticación mutua de forma que tanto el usuario como el servidor verifican su identidad mutuamente. Para garantizar seguridad, los mensajes del protocolo Kerberos están protegidos contra el espionaje y ataque por réplica.

El ***Inicio de sesión único (SSO)*** permite conectarse una vez y acceder a múltiples sistemas de software relacionados pero que al mismo tiempo son independientes, sin necesidad de loguearse de nuevo. Cuando se ingresa con Windows usando un Directorio activo, se nos asigna un token, el cual puede luego ser usado para ingresar en otros sistemas automáticamente.

Finalmente, el Directorio activo permite organizar todos los recursos de red (incluyendo usuarios, grupos, impresoras, equipos de cómputo y otros objetos) de manera que puede asignar contraseñas, permisos, derechos, etcétera, a la identidad que así lo requiera. Puede también asignar a quién le está permitido manejar un grupo de objetos.

▶ *Análisis de los controladores de dominio*

Un ***controlador de dominio*** es un servidor de Windows que almacena una réplica de la cuenta y de la información de seguridad de un dominio y define los límites del mismo. Para hacer que un equipo de cómputo que ejecuta Windows Server 2008 sea un controlador de dominio, primero tiene que instalar Servicios de Dominio del Directorio activo. Luego tiene que ejecutar el comando dcpromo (forma corta de promoción dc) para hacer que el servidor sea un controlador de dominio desde los cuadros de dialogo de Buscar programas y archivos, o desde el símbolo del sistema.

Después de que un equipo de cómputo ha sido promovido a controlador de dominio, hay varias consolas de complemento MMC para manejar el Directorio activo, incluyendo:

- **Usuarios y Equipos de cómputo de Directorio activo**: Utilizado para administrar usuarios, grupos, equipos de cómputo y unidades organizacionales.
- **Dominios y Confianzas del Directorio activo**: Usar para administrar confianzas de dominio, niveles funcionales de dominio y de bosque y sufijos del nombre principal de usuario (UPN).
- **Sitios y Servicios de Directorio activo**: Usado para administrar la replicación de los datos del directorio entre todos los sitios en un bosque de Servicios de Dominio de Directorio activo (AD DS).
- **Centro Administrativo de Directorio activo:** Usado para administrar y publicar información en el directorio, incluyendo la administración de usuarios, grupos, equipos de cómputo, dominios, controlador de dominios y unidades organizacionales. El centro Administrativo del Directorio activo es nuevo en Windows Server 2008 R2.
- **Consola de Gestión de Políticas de Grupos (GPMC)**: Proporciona una sola herramienta administrativa para la gestión de las Políticas de Grupos a través de la empresa. La GPMC está instalada automáticamente en Windows Server 2008 y se necesita descargar e instalar un controlador de dominios más nuevo en el controlador de dominios de Windows Server 2003. Aunque estas herramientas están instaladas por lo general en el controlador de dominios, también pueden ser instaladas en las PC del cliente de manera que pueda manejar el Directorio activo sin necesidad de conectarse a un controlador de dominio.

El Directorio activo usa replicación multi-maestra lo cual significa que no hay un controlador maestro de dominio, usualmente referido como controlador principal de dominio en Windows NT. Sin embargo, existen ciertas funciones que sólo pueden ser manejadas por un controlador de dominio a la vez.

Una de las funciones es el emulador de PDC, que proporciona compatibilidad con versiones anteriores de clientes NT4, que es poco común. Sin embargo, también actúa como la autoridad principal para los cambios de contraseña y como servidor maestro de tiempo dentro del dominio.

Un servidor que no está siendo ejecutado como un controlador de dominio se conoce como un ***servidor miembro***. Para degradar un controlador de dominio a un servidor miembro, debe volver a ejecutar el programa de dcpromo.

Introducción a NTLM

Aunque Kerberos es el protocolo de autenticación predeterminado para los equipos de cómputo de dominio actuales, ***NTLM*** es el protocolo de autenticación predeterminado para Windows NT, equipos de cómputo independientes que no forman parte de un dominio y situaciones en las que estás autenticando en un servidor usando una dirección IP. NTLM también actúa como un protocolo de autenticación de caída si la autenticación por Kerberos no puede ser realizada, tal como cuando se bloquea por un firewall.

NTLM usa un mecanismo de "challenge-response" para el proceso de autenticación en el que los clientes son habilitados para probar sus identidades sin enviar una contraseña al servidor. Después de que un "challenge message" de ocho bytes se envía al cliente desde el servidor, el cliente usa la contraseña del usuario como clave para generar una respuesta que regresa al servidor utilizando un algoritmo *hash* MD4/MD5 (cálculo matemático en un sentido) y encriptación DES (un algoritmo de encriptación generalmente usado que cifra y descifra datos con la misma clave).

Introducción a Kerberos

Con Kerberos, la seguridad y autenticación se basan en una tecnología de clave secreta y cada host en la red tiene la suya. El Centro de Distribución de Claves mantiene una base de datos de estas claves secretas.

Cuando un usuario entra en un recurso de red por medio de Kerberos, el cliente transmite el nombre de usuario al servidor de autenticación, junto con la identidad del servicio al que quiere conectarse (por ejemplo, un servidor de archivos). El servidor de autenticación construye un pase de entrada, el cual genera de manera aleatoria una clave encriptada con la clave secreta del servidor de archivos y la envía al cliente como parte de sus credenciales, las cuales incluyen la clave de sesión cifrada con la clave del cliente. Si el usuario escribe la contraseña correcta, entonces el cliente puede descifrar la clave de sesión, presentar el pase de entrada al servidor de archivos y dar al usuario la clave secreta compartida de sesión para comunicarse entre sí. Los pases de entrada son marcados con la hora y generalmente tienen un periodo de expiración sólo de unas horas.

Para que todo esto funcione y se garantice la seguridad, el controlador de dominios y clientes deben estar a la misma hora. Los sistemas operativos de Windows incluyen la herramienta de Servicio de Tiempo (W32Time service). La autenticación por Kerberos funcionará si el intervalo de tiempo entre los equipos de cómputo en cuestión se encuentra dentro de la variación de tiempo máxima habilitada. Lo predeterminado son cinco minutos. Puede también apagar la herramienta de Servicio de Tiempo e instalar un servicio de tiempo de terceros. Desde luego, si tiene problemas autenticando, debe asegurarse de que la hora es la correcta para el controlador de dominios y el cliente que está teniendo el problema.

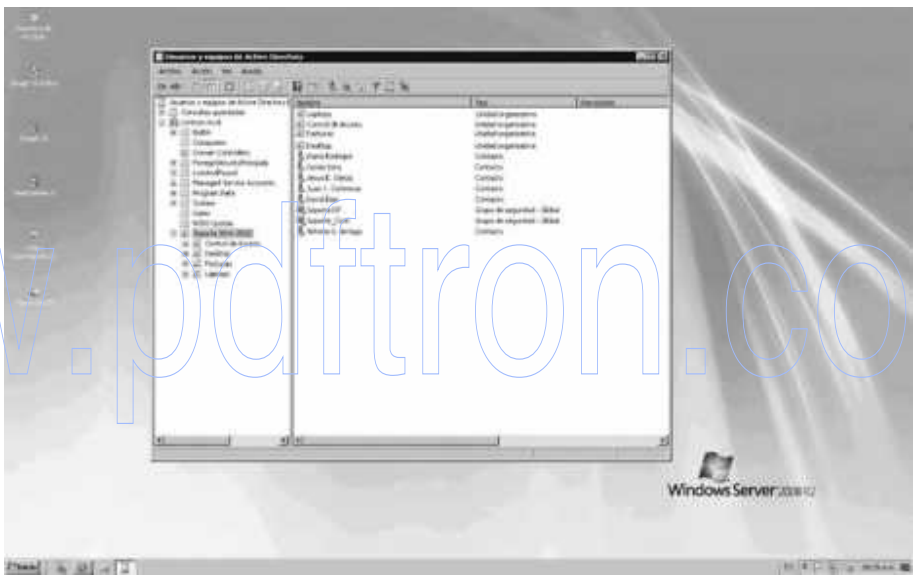
Unidades organizacionales

Como se ha mencionado con anterioridad, una organización puede tener miles de usuarios y miles de equipos de cómputo. Con Windows NT, el dominio podría manejar algunos objetos antes de que surjan algunos problemas de rendimiento. Con versiones posteriores de Windows, sin embargo, el tamaño del dominio ha aumentado dramáticamente. Mientras que con Windows NT podría requerir varios dominios para definir a su organización, ahora usted puede tener solamente un dominio para representar a una organización grande. Sin embargo, si tiene miles de estos objetos, aún puede requerir una forma de organizarlos y administrarlos.

Para ayudar a organizar objetos dentro de un dominio y minimizar el número de dominios, puede usar ***unidades organizacionales***, u OU, las cuales pueden ser usadas para sostener usuarios, grupos, equipos de cómputo y otras unidades organizacionales. Ver Figura 2-3. Una unidad organizacional puede sólo contener objetos que están localizados en un dominio. Aunque no existen restricciones en cuanto a cuantas OU anidadas (una OU dentro de otra OU) puede tener, se debe diseñar una jerarquía superficial para un mejor rendimiento.

Figura 2-3

Unidad organizacional de Active Directory



Cuando se instala el Directorio activo por primera vez, hay varias unidades organizacionales ya creadas. Incluyen equipos, usuarios, controladores de dominio y unidades organizacionales incorporadas. A diferencia de las unidades organizacionales que se puedan crear, estas unidades organizacionales no permiten delegar permisos o asignar las políticas de grupo (las políticas de grupo se explicarán más adelante en el texto.) Los contenedores son objetos que pueden almacenar o contener otros objetos. Incluyen el bosque, árbol, dominio y la unidad organizacional. Para ayudarle a gestionar los objetos, se puede delegar autoridad a un contenedor, sobre todo en el dominio o unidad organizacional.

Por ejemplo, supongamos que tiene su dominio dividido por ubicación física. Puede asignar un control autoritario de administrador del sitio a la OU que representa una ubicación física determinada y el usuario sólo tendrá el control administrativo sobre los objetos dentro de esa OU. También puede estructurar sus unidades organizacionales por función o áreas de gestión. Por ejemplo, podría crear una OU de ventas para contener a todos los usuarios de ventas. También podría crear una OU de impresoras para contener todos los objetos de estas y, a continuación, asignarle un administrador.

De manera similar a NTFS y el registro, puede asignar permisos a usuarios y grupos sobre un objeto de Active Directory. Sin embargo, normalmente podría delegar el control a un usuario o grupo. Puede asignar tareas administrativas básicas a usuarios o grupos regulares y dejar la administración de todo el dominio y de todo el bosque a los miembros de los grupos de Administradores de dominio y administradores de empresa. Al delegar la administración, se permite que los grupos dentro de tu organización tengan un mayor control de sus recursos de la red local. También ayuda a proteger la red de daños accidentales o maliciosos limitando el número de miembros de los grupos de administradores.

Puede delegar el control administrativo a cualquier nivel de un árbol de dominios creando unidades organizacionales dentro de un dominio y, a continuación, delegar el control administrativo para las unidades organizacionales específicas para determinados usuarios o grupos.

→ Delegar el Control

PREPÁRESE. Para delegar el control de una unidad organizacional, realice los siguientes pasos:

1. Abrir **Usuarios y equipos de Directorio activo**.
2. En el árbol de la consola, hacer clic en la unidad organizacional a la que desea delegar el control.
3. Haga clic en **Delegar control** para iniciar el Asistente para Delegar el Control y, a continuación, siga las instrucciones.

► *Análisis de los objetos*

Un objeto es un distintivo, conjunto de atributos o características que representan un recurso de red con nombre. Los objetos comunes utilizados dentro de un Directorio activo son equipos, usuarios, grupos e impresoras. Los atributos tienen valores que definen el objeto específico. Por ejemplo, un usuario podría tener el nombre Juan, el apellido Pérez y jperez como nombre de inicio de sesión, y así todos identifican al usuario.

Cuando se trabaja con objetos, los administradores suelen utilizar los nombres de esos objetos, tales como nombres de usuario. Sin embargo, a todos los objetos del Directorio activo también se les asigna un número único de 128 bits, llamado un Security Identifier (SID), a veces se denomina Globally Unique Identifier (GUID), para identificarlos de forma única. Por lo tanto, si alguien cambia su nombre de usuario, puede cambiar ese nombre en la red, pero él o ella podrán acceder a todos los mismos objetos y tener todos los mismos derechos que antes poseían porque esos objetos y derechos se asignan al GUID.

Los GUID también proporcionan cierta seguridad si un usuario se borra. No puede crear una nueva cuenta con el mismo nombre de usuario y esperar tener acceso a todos los objetos y todos los derechos que tenía anteriormente. Por el contrario, si decide dejar ir a alguien de su organización y más tarde sustituye a esa persona, debe en su lugar desactivar la cuenta de la primera persona, contratar a la nueva persona, cambiar el nombre de la cuenta de usuario, cambiar la contraseña y volver a activarla. De este modo, la nueva persona será capaz de acceder a todos los mismos recursos y tener todos los mismos derechos que el usuario anterior tenía.

El esquema de Directorio activo define el formato de cada objeto y los atributos o los campos de cada objeto. El esquema predeterminado contiene definiciones de objetos comúnmente usados como cuentas de usuario, equipos de cómputo, impresoras y grupos.

Por ejemplo, el esquema define que la cuenta de usuario tiene campos de nombre, apellido y números telefónicos.

Para permitir que el Directorio activo sea flexible para que pueda soportar otras aplicaciones, se puede extender un esquema para incluir atributos adicionales. Por ejemplo, puede agregar número de insignia o campos de identificación de empleado al objeto de usuario. Al instalar algunas aplicaciones, como Microsoft Exchange, éstas extienden el esquema, por lo general mediante la adición de atributos adicionales o campos para poder soportar la aplicación.

Examinar los usuarios

Una ***cuenta de usuario*** permite a una persona iniciar sesión en un equipo y dominio. Como resultado, se puede utilizar para probar la identidad de un usuario, y así después poder determinar qué usuario puede acceder y qué tipo de acceso tendrá el usuario (autorización). Las cuentas de usuario también pueden utilizarse para la auditoría. Por ejemplo, si hay un problema de seguridad en el que hubo un acceso inapropiado o borrado, los datos de la cuenta de usuario pueden utilizarse para mostrar quién entró o eliminó el objeto.

En las redes de Windows de hoy en día, existen dos tipos de cuentas de usuario:

- Cuenta de usuario local
- Cuenta de usuario de dominio

Una cuenta de usuario permite iniciar sesión y acceder a la computadora donde se creó la cuenta. La ***cuenta de usuario local*** se almacena en la base de datos del ***Security Account Manager (SAM)*** en el equipo local. El único equipo de Windows que no dispone de una base de datos SAM es el controlador de dominio. La cuenta de usuario local de administrador es la única cuenta que se crea y es habilitada de forma predeterminada en Windows. Aunque no se puede eliminar esta cuenta, se puede cambiar el nombre.

La otra cuenta creada de forma predeterminada es la cuenta de invitado. Fue diseñado para el usuario ocasional que necesita tener acceso a recursos de red en una red de baja seguridad. La cuenta de usuario local de invitado está deshabilitada de forma predeterminada y no se recomienda para uso general.

Una cuenta de ***usuario de dominio*** se almacena en el controlador de dominio y permite obtener acceso a los recursos dentro del mismo, suponiendo que ha concedido permisos para tener acceso a esos objetos. La cuenta de usuario de administrador de dominio es la única cuenta que se crea y es habilitada de forma predeterminada en Windows, cuando se crea uno. Una vez más, aunque no se puede eliminar esta cuenta, se puede cambiar el nombre.

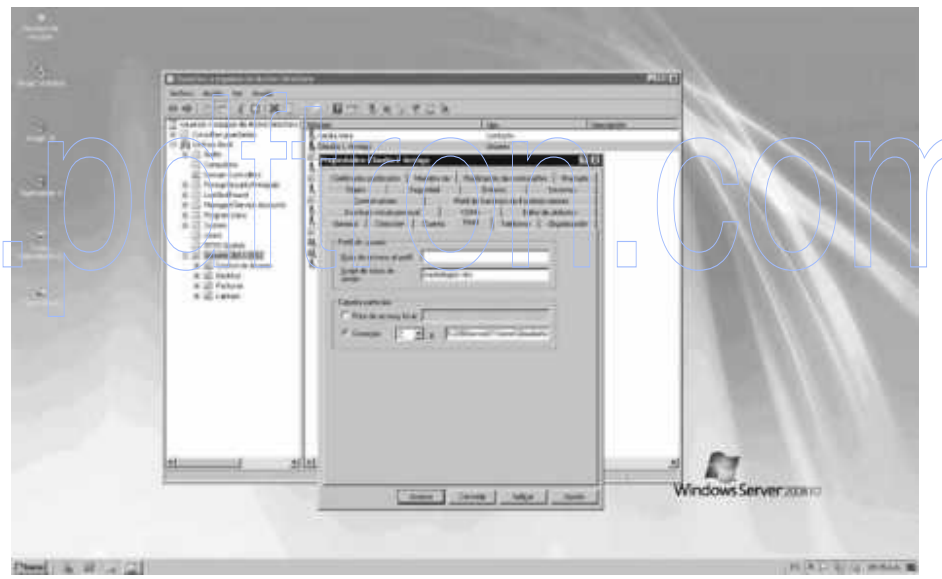
Cuando se crea una cuenta de usuario de dominio, debe proporcionarse un nombre, apellido y un nombre de inicio de sesión de usuario. El nombre de inicio de sesión de usuario debe ser único con el dominio. Ver la figura 2-4. Después de crear la cuenta de usuario, puede, a continuación, abrir las propiedades de la cuenta de usuario y configurar el nombre, la hora de inicio de sesión, los números de teléfono y las direcciones de los equipos con los que el usuario puede iniciar sesión, de qué grupos la persona es miembro y así sucesivamente. También puede especificar si una contraseña caduca, si se puede cambiar y si una cuenta está deshabilitada. Por último, en la pestaña de perfil, puede definir el directorio principal del usuario, la secuencia de comandos de inicio de sesión y la ruta del perfil del usuario. Ver la figura 2-5.

Figura 2-4

Cuenta del usuario en Active Directory

Figura 2-5

Pestaña de Perfil



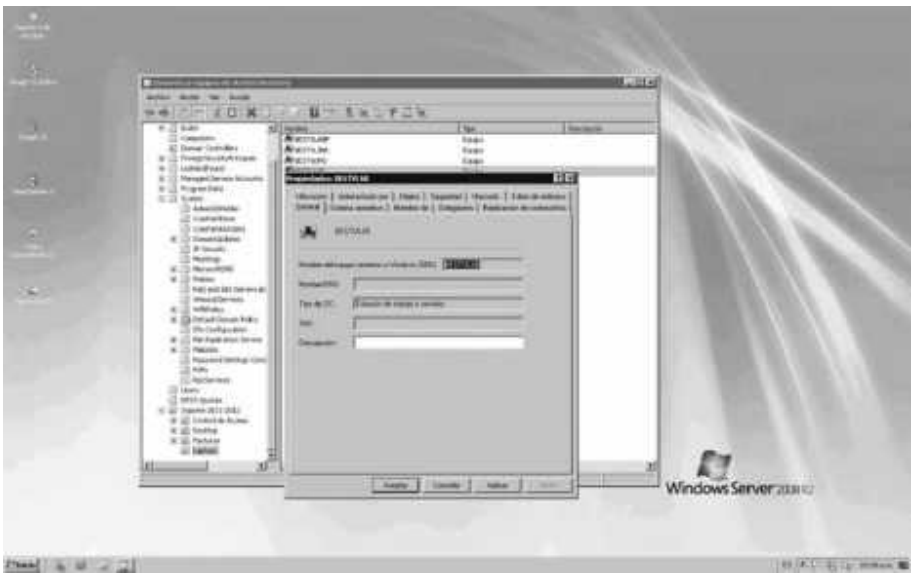
Análisis de los equipos

Como las cuentas de usuario, las ***cuentas de equipo*** de Windows proporcionan un medio para autenticar y auditar el acceso de un equipo a una red de Windows, así como su acceso a los recursos del dominio. Cada equipo de Windows para el que desee conceder acceso a los recursos debe tener una cuenta de equipo único. Estas cuentas también pueden utilizarse para efectos de auditoría, debido a que especifican qué sistemas se utilizaron para tener acceso a los recursos específicos.

Ver la figura 2-6.

Figura 2-6

Cuenta de equipo



Qué son los grupos

Un *grupo* es una colección o lista de cuentas de usuario o de equipo. A diferencia de un contenedor, un grupo no almacena usuarios o equipos; más bien, sólo los enumera. El uso de grupos puede simplificar la administración, sobre todo cuando se trata de asignar derechos y permisos.

Un grupo se utiliza para agrupar usuarios y equipos de modo que al asignar derechos y permisos, se asignan al grupo en lugar de a cada usuario individual. Usuarios y equipos pueden ser miembros de varios grupos, y en algunos casos, se puede designar un grupo como parte de otro.

Examen de los tipos de grupos

En el Directorio activo de Windows, hay dos tipos de grupos: seguridad y distribución. Un grupo de seguridad se utiliza para asignar derechos y permisos y para obtener acceso a recursos de red. También puede utilizarse como un grupo de distribución. Un grupo de distribución es empleado sólo para funciones que no sean de seguridad, tales como la distribución de correo electrónico, y no puede utilizarse para asignar derechos y permisos.

Examen de los alcances del grupo

Cualquier grupo, ya sea de seguridad o de distribución, se caracteriza por un alcance que identifica el grado al que aplica el grupo en el árbol de dominios o en el bosque. Los tres alcances del grupo son los siguientes:

- **Local**: contiene los grupos globales y universales, a pesar de que también puede contener cuentas de usuario y otros grupos locales de dominio. Un grupo local de dominio usualmente está con el recurso al que se desea asignar los permisos o derechos.
- **Global**: diseñado para contener cuentas de usuario, aunque también puede contener otros grupos globales, los cuales están diseñados para ser de "control

total" o "generales" para un dominio. Después de colocar las cuentas de usuario en grupos globales, estos se colocan normalmente en grupos locales de dominio o Universales.

- **Universal**: diseñado para contener grupos globales de varios dominios, aunque también puede contener otros grupos universales y cuentas de usuario. Porque los catálogos globales replican la pertenencia al grupo universal, se debe limitar la pertenencia a grupos globales. De esta forma, si cambia un miembro dentro de un grupo global, el catálogo general no tendrá que replicar el cambio.

Ver la tabla 2-1.

Tabla 2-1
Alcances del grupo

Alcance	Los miembros pueden incluir:	Los permisos de los miembros pueden ser asignados…	El alcance del grupo puede convertirse en…
Universal	Cuentas de cualquier dominio del bosque en el que reside este grupo universal. Grupos globales de cualquier dominio del bosque en el que reside este grupo universal. Grupos universales de cualquier dominio del bosque en el que reside este grupo universal.	En cualquier dominio o bosque.	Dominio local. Global (siempre y cuando no haya otros grupos universales existentes como miembros).
Global	Cuentas del mismo dominio que el grupo global principal. Grupos globales del mismo dominio que el grupo global principal.	En cualquier dominio.	Universal (siempre que el grupo no sea un miembro de cualquier otro grupo global).
Dominio local	Cuentas de cualquier dominio, grupos globales de cualquier dominio, grupos universales de cualquier dominio y dominio de grupos locales, pero sólo del mismo dominio que el dominio del grupo local principal.	Sólo dentro del mismo dominio que el dominio del grupo local principal.	Universal (siempre que no haya otros grupos locales de dominio existentes como miembros).

Al asignar derechos y permisos, debe intentarse siempre colocar a los usuarios en grupos y asignar los derechos y permisos a estos en lugar de a los usuarios individuales. Para gestionar con eficacia el uso global y el dominio de los grupos locales cuando se asigna el acceso a recursos de la red (recuerda que el mnemónico es AGDLP [accounts, global, domain local, permissions]):

- En primer lugar, agregue a la cuenta de usuario (A) en el grupo global (G) en el dominio donde el usuario existe.
- A continuación, agregue el grupo global (G) desde el dominio de usuario en el dominio del grupo local (DL) en el dominio de recursos.

- Por último, asigne permisos (P) en el recurso para el grupo local (DL) en su dominio.
- Si utiliza los grupos universales, el mnemónico extendido es AGUDLP:
- En primer lugar, agregue la cuenta de usuario (A) en el grupo global (G) en el dominio donde el usuario existe.
- A continuación, agregue el grupo global (G) desde el dominio del usuario en el grupo universal (U).
- A continuación, agregue el grupo universal (U) al dominio del grupo local (DL).
- Por último, asigne permisos (P) en el recurso para grupo local (DL) en su dominio.

Grupos integrados

De forma similar a las cuentas de administrador y de invitado, Windows tiene grupos predeterminados llamados ***grupos integrados***. A estos grupos predeterminados se les ha concedido los derechos esenciales y permisos para comenzar. Algunos de los grupos integrados de Windows son los siguientes:

- **Administrador del dominio**: Los miembros de este grupo pueden realizar tareas administrativas en cualquier equipo dentro del dominio. De forma predeterminada, la cuenta de administrador es un miembro.
- **Los usuarios del dominio**: Windows agrega automáticamente cada nueva cuenta de usuario de dominio al grupo correspondiente.
- **Operadores de cuentas**: Los miembros de este grupo pueden crear, eliminar y modificar cuentas de usuario y grupos.
- **Los operadores de copia de seguridad**: Los miembros de este grupo pueden realizar copias de seguridad y restaurar todos los controladores de dominio mediante el comando Copias de seguridad de Windows.
- **Usuarios autenticados**: Este grupo incluye a todos los usuarios con una cuenta de usuario válida en el equipo o en el Directorio activo. Utiliza el grupo de usuarios autenticados en lugar de todos los del grupo para evitar el acceso anónimo a un recurso.
- **Todos**: Este grupo incluye a todos los usuarios que acceden a un equipo con una cuenta de usuario válida.

Para obtener más información sobre los grupos disponibles, visitar el siguiente sitio Web:

http://technet.Microsoft.com/en-US/Library/cc756898(WS.10).aspx

← *Buscar la autenticación del servidor Web*

Cuando una persona tiene acceso a un servidor web, como aquellos que ejecutan en Microsoft´s Internet Information Server (IIS), puede utilizar varios métodos de autenticación.

Cuando se autentican los servidores web, el IIS proporciona una variedad de esquemas de autenticación:

- **Anónimo (activado por defecto)**: La autenticación anónima proporciona a los usuarios acceso a un sitio Web sin que se les pida un nombre de usuario o contraseña. En su lugar, el IIS utiliza una cuenta de usuario de Windows especial llamada IUSR_ *machinename* para el acceso. De manera predeterminada, el IIS controla la contraseña para esta cuenta.

- **Básica**: La autenticación básica solicita al usuario un nombre de usuario y una contraseña. Sin embargo, incluso aunque el nombre de usuario y la contraseña se envían como codificación Base64, es enviado básicamente en texto sin formato ya que la codificación Base64 se utiliza como un formato y no como un encriptado. Si necesita encriptar los nombres de usuario y contraseñas mientras utilizas la autenticación básica, puedes utilizar los certificados digitales para que esta información se encripte con https.
- **Implícita**: La autenticación implícita es un mecanismo de challenge/response que envía un resumen o un hash de la contraseña como clave en lugar de enviar la contraseña a través de la red.
- **Autenticación integrada de Windows**: La autenticación de Windows integrada (anteriormente conocida como la autenticación NTLM y autenticación challenge/response de Windows NT) puede utilizar autenticación NTLM o Kerberos V5.
- **Asignación de certificados de cliente**: La asignación de certificados de cliente utiliza un certificado digital que contiene información sobre una entidad y la clave pública de la misma para fines de autenticación.

▪ Comparar los derechos y permisos

↓ EN RESUMEN

Lo que un usuario pueda hacer en un sistema o a un recurso está determinado por dos cosas: derechos y permisos.

☑ Listo para la Certificación

¿Puede describir cómo se almacenan los permisos para un objeto?
—2.2

Un *derecho* autoriza a un usuario a realizar determinadas acciones en un equipo, como el inicio de sesión en un sistema de forma interactiva o copias de seguridad de archivos y directorios en un sistema. Los derechos de usuario se asignan a través de las políticas locales o de las de grupo del Directorio activo. Ver la figura 2-7.

Figura 2-7

Políticas del grupo para asignar los derechos de usuario

Un ***permiso*** define el tipo de acceso que se concede a un objeto (un objeto puede ser reconocido con un identificador de seguridad) o atributo. Los objetos más comunes a los que se asignan permisos son los archivos NTFS y las carpetas, impresoras y objetos del Directorio activo. La información acerca de qué usuarios pueden acceder a un objeto y lo que pueden hacer se almacena en la ***Access control list (ACL)***, que enumera todos los usuarios y grupos que tienen acceso a él. Los permisos NTFS y de impresoras se discuten en la lección siguiente.

▪ Análisis de NTFS

↓ EN RESUMEN

Un sistema de archivos es un método que almacena y organiza archivos informáticos y los datos que contienen. También mantiene la ubicación física de los archivos para que fácilmente se puedan encontrar y acceder a los archivos en el futuro. Windows Server 2008 soporta sistemas de archivos FAT16, FAT32 y NTFS en unidades de disco duro.

Después de particionar un disco, a continuación, se debe formatear (puedes formatear el disco como FAT16, FAT32 o NTFS). De estos, ***NTFS*** es el sistema de archivos preferido para los sistemas operativos actuales.

FAT16, a veces llamado genéricamente como File Allocation Table (FAT), es un sistema simple de archivos que utiliza memoria mínima y se ha utilizado con DOS. Originalmente soportaba el esquema de asignación de nombres 8.3, lo que permitía nombres de archivo de hasta ocho caracteres y la extensión de nombre de archivo de tres. Más tarde, se fue revisado para apoyar los nombres de archivo largos. Lamentablemente, los volúmenes FAT sólo pueden admitir hasta 2 GB.

FAT32 fue lanzado con el segundo gran lanzamiento de Windows 95. A pesar de que este sistema de archivos puede soportar unidades más grandes, el Windows de hoy soporta volúmenes hasta de 32 GB. También admite nombres de archivo largos.

Hoy en día, NTFS es el sistema de archivos preferido, ya que soporta ambos volúmenes hasta 16 exabytes y nombres de archivo largos. Además, NTFS es más tolerante que los sistemas anteriores de archivo utilizados en Windows porque es un sistema de archivos de journal o registro por diario. Un sistema de archivos journal asegura que una transacción se escribe en el disco correctamente antes de ser reconocida. Por último, NTFS ofrece mayor seguridad a través de permisos y encriptado.

▶ *Permisos de NTFS*

Los ***Permisos NTFS*** permiten controlar qué usuarios y grupos puede tener acceso a archivos y carpetas en un volumen NTFS. La ventaja con los permisos NTFS es que afectan a usuarios locales y a usuarios de la red.

Por lo general, al asignar permisos NTFS, tendrían que asignarse los permisos estándares siguientes:

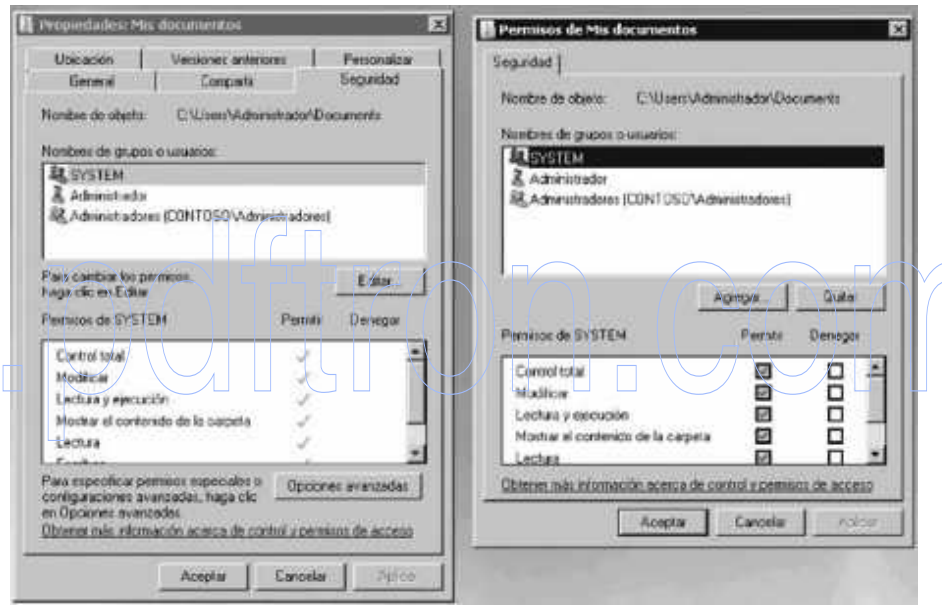
- **Control total**: Permiso para leer, escribir, modificar y ejecutar los archivos en una carpeta, cambiar atributos y permisos y hacer uso de la carpeta o los archivos que contiene.
- **Modificar**: Permiso para leer, escribir, modificar y ejecutar los archivos en la carpeta, así como para cambiar los atributos de la carpeta o archivos que contiene.

- **Leer y ejecutar**: Permiso para mostrar el contenido de una carpeta; para mostrar los datos, atributos, propietario y permisos para los archivos dentro de la carpeta; y para ejecutar archivos dentro de la carpeta.
- **Lista de contenido de la carpeta**: Permiso para mostrar el contenido de una carpeta, así como mostrar los datos, atributos, propietario y permisos para los archivos dentro de la carpeta.
- **Lectura**: Permiso para mostrar datos de un archivo, atributos, propietario y permisos.
- **Escribir**: Permiso para escribir en un archivo, añadir al archivo y leer o cambiar los atributos del archivo.

Para administrar los permisos de NTFS, puede hacer clic derecho en una unidad, carpeta o archivo y seleccionar Propiedades y, a continuación, seleccionar la pestaña de Seguridad. Como se muestra en la figura 2-8, deberá ver el grupo y los usuarios que tienen permisos de NTFS y sus respectivos permisos de NTFS estándar. Para cambiar los permisos, debes hacer clic en el botón Editar.

Figura 2-8

Permisos NTFS



Los grupos o usuarios a los que se le concede el permiso de Control total sobre una carpeta pueden eliminar cualquier archivo independientemente de los permisos que se solicitan para protegerlo. Además, la función de mostrar el contenido de la carpeta, es heredada por las carpetas pero no por los archivos y sólo deberá constar al ver los permisos de esta. En Windows Server 2008, el grupo Todos no incluye el grupo de Inicio de sesión anónimo de forma predeterminada, por lo que los permisos que se aplican para el grupo Todos no afectan al grupo Inicio de sesión anónimo.

Para simplificar la administración, se recomienda que conceda permisos mediante grupos. A través de la asignación de permisos NTFS a un grupo, se les estaría otorgando permisos a una o más personas, reduciendo el número de entradas en cada lista de acceso y reduciendo la cantidad de esfuerzo para configurar situaciones en que varias personas necesitan tener acceso a determinados archivos o carpetas.

Permisos efectivos de NTFS

La estructura de carpetas/archivos en una unidad NTFS puede ser muy complicada e incluye muchas carpetas y subcarpetas. Además, debido a que se recomienda asignar permisos a grupos y a diferentes niveles en un volumen NTFS, conocer los permisos efectivos de una determinada carpeta o archivo para un usuario en particular puede ser complicado.

Hay dos tipos de permisos utilizados en NTFS:

- ***Permisos explícitos***: Permisos concedidos directamente a un archivo o carpeta.
- ***Permisos heredados:*** Permisos concedidos a una carpeta (objeto o contenedor primario) que transmiten a los objetos secundarios (archivos o subcarpetas) que se encuentra dentro.

Al asignar permisos a una carpeta, por defecto, se aplican tanto a la carpeta como a las subcarpetas y archivos dentro de ella. Para detener los permisos heredados, puede seleccionar la casilla "Reemplazar todos los permisos de objetos secundarios por permisos heredables de este objeto" en el cuadro de diálogo de Configuración de seguridad avanzada. A continuación, se le preguntará si está seguro de que desea continuar. También puede deseleccionar la casilla "Incluir todos los permisos heredables del objeto primario de este objeto". Cuando esta casilla está vacía, Windows mostrará un cuadro de diálogo de seguridad. Al hacer clic en el botón Copiar, el permiso explícito se copiará de la carpeta principal a la subcarpeta o archivo. A continuación, puede cambiar los permisos explícitos en la subcarpeta o archivo. Si hace clic en el botón Eliminar, se retira el permiso heredado por completo.

De forma predeterminada, los objetos dentro de una carpeta heredan los permisos de cuando se crean. Sin embargo, los permisos explícitos tienen prioridad sobre los heredados. Así que, si concede diferentes permisos a un nivel inferior, el menor nivel de permisos tiene prioridad.

Por ejemplo, supongamos que tiene una carpeta llamada Datos. Dentro de la carpeta de Datos, usted tiene la Carpeta1, y dentro de la Carpeta1, tiene la Carpeta2. Si usted concede Permitir el control total a una cuenta de usuario, el permiso Permitir control total se pasará a las subcarpetas y archivos dentro de la carpeta de Datos.

Objeto	Permisos NTFS
Datos	Permite Permiso de Control Total (explícito)
Carpeta 1	Permite Control Total (heredado)
Carpeta 2	Permite Control Total (heredado)
Archivo 1	Permite Control Total (heredado)

Por lo tanto, si concede Permitir un Control Total en la carpeta Datos para una cuenta de usuario, el Permiso de Control Total normalmente afectará a la Carpeta 1. Sin embargo, si concede Permiso de Lectura a la carpeta 1 en la misma cuenta de usuario, el permiso Permitir leer sobrescribirá el permiso heredado y también se transmitirá a la carpeta 2 y al archivo 1.

Objeto	Permisos NTFS
Datos	Permite Permiso de Control Total (explícito)
Carpeta 1	Permitir la lectura (explícito)
Carpeta 2	Permitir la lectura (heredado)
Archivo 1	Permitir la lectura (heredado)

Si un usuario tiene acceso a un archivo, ese usuario podrá seguir teniendo acceso al archivo, incluso si él o ella no tienen acceso a la carpeta que contiene el archivo. Por supuesto, porque el usuario no tiene acceso a la carpeta, el usuario no puede desplazarse o navegar a través de la carpeta para obtener el archivo. Por lo tanto, el usuario tendría que utilizar el Universal Naming Convention (UNC) o la ruta de acceso local para abrir el archivo.

Estos son los diferentes tipos de permiso que tendrá:

- **Check con marca**: Aquí, se han asignado explícitamente los permisos.
- **Check sin marca**: Aquí, no hay permisos asignados.
- **Sombreados**: Aquí, se conceden permisos a través de la herencia de una carpeta principal.

Además de conceder Permitir permisos, también se puede Denegar permisos, el cual siempre reemplaza a los otros permisos que se hayan concedido, incluidas las situaciones en las que a un usuario o grupo se le haya dado un Control total. Por ejemplo, si a un grupo le han sido concedidos permisos de Leer y Escribir pero a uno de los miembros del grupo se le ha denegado el permiso de escritura, los derechos efectivos de ese usuario sólo incluyen el permiso de lectura.

Cuando se combina aplicar Denegar permisos frente a Permitir permisos y permisos explícitos versus permisos heredados, la jerarquía de la precedencia es la siguiente:

1. Denegación Explícita
2. Permitir Explícito
3. Denegación Heredada
4. Permitir Heredado

Debido a que los usuarios pueden ser miembros de varios grupos, es posible que tengan varios conjuntos de permisos explícitos para una carpeta o archivo. Cuando esto ocurre, los permisos se combinan para formar los ***permisos efectivos***, que son los permisos reales al iniciar sesión y acceder a un archivo o carpeta. Se componen de los permisos explícitos más cualquier permiso heredado.

Al calcular los permisos efectivos, debe calcular en primer lugar los permisos explícitos y heredados para un individuo o grupo y, a continuación, combinarlos. Cuando se combinan permisos de usuario y de grupo para la seguridad NTFS, el permiso efectivo es el permiso acumulativo. La única excepción es que siempre se aplica Denegar permisos.

Por ejemplo, supongamos que tiene una carpeta llamada Datos. Dentro de la carpeta Datos, tienes una Carpeta 1 y, a continuación, dentro de la Carpeta 1, tiene una Carpeta 2. Imaginemos también que el Usuario 1 es un miembro del Grupo 1 y del Grupo 2. Si asigna el permiso Permitir escribir a la carpeta Datos para el Usuario 1, el Permitir lectura a la Carpeta 1 del Grupo 1 y el permiso Permitir modificar a la Carpeta 2 para el Grupo 2, entonces los permisos efectivos del usuario 1 serían como se muestra a continuación:

Objeto	Permisos de NTFS de usuario 1	Permisos de grupo 1	Permisos de grupo 2	Permisos efectivos
Datos	Permiso de Permitir escritura (explícito)			Permiso de permitir escritura
Carpeta 1	Permiso de Permitir escritura (heredado)	Permiso de Permitir lectura (explícito)		Permiso de Permitir lectura y escritura
Carpeta 2	Permiso de Permitir escritura (heredado)	Permiso de Permitir lectura (heredado)	Permiso de Permitir modificar (explícito)	Permiso de Permitir modificar
Archivo 1	Permiso de Permitir escritura (heredado)	Permiso de Permitir lectura (heredado)	Permiso de Permitir modificar (heredado)	Permiso de Permitir modificar *

* El permiso de Modificar incluye los permisos de Lectura y Escritura.

Ahora, supongamos que tiene una carpeta llamada Datos. Dentro de la carpeta Datos, usted tienes la Carpeta 1 y dentro de la Carpeta 1, tienes la Carpeta 2. El Usuario 1 es un miembro del Grupo 1 y del Grupo 2. Asigna el permiso Permitir escribir a la carpeta Datos del Usuario 1, el permiso Permitir leer a la Carpeta 1 del Grupo 1 y el permiso Denegar modificar a la Carpeta 2 para el grupo 2. Aquí, los permisos efectivos del usuario1 serían los siguientes:

Objeto	Permisos de NTFS de usuario 1	Permisos de grupo 1	Permisos de grupo 2	Permisos efectivos
Datos	Permiso de Permitir escritura (explícito)			Permiso de Permitir escritura
Carpeta 1	Permiso de Permitir escritura (heredado)	Permiso de Permitir lectura (explícito)		Permiso de Permitir lectura y escritura
Carpeta 2	Permiso de Permitir escritura (heredado)	Permiso de Permitir lectura (heredado)	Permiso de Denegar modificación (explícito)	Permiso de Denegar modificación
Archivo 1	Permiso de Permitir escritura (heredado)	Permiso de Permitir lectura (heredado)	Permiso de Denegar modificación (heredado)	Permiso de Denegar modificación

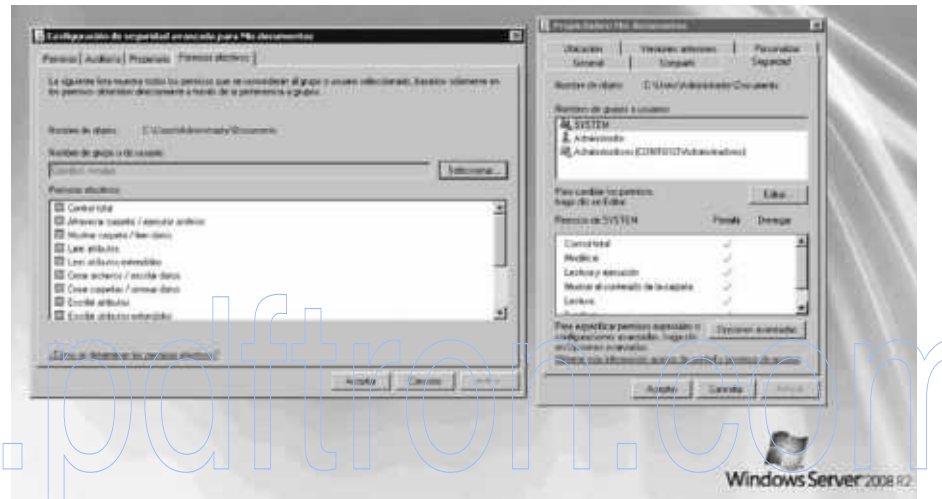
→ Ver permisos efectivos de NTFS

PREPÁRESE. Para ver los permisos efectivos de NTFS concedidos a un usuario de un archivo o carpeta, realice los pasos siguientes:

1. Haga clic derecho en el archivo o carpeta y selecciona **Propiedades**.
2. Seleccione la pestaña de **Seguridad**.
3. Haga clic en el botón **Opciones avanzadas**.
4. Haga clic en la pestaña **Permisos efectivos**.
5. Haga clic en el botón **Seleccionar** y escriba el nombre del usuario o grupo que desea ver. Dé clic en el botón **Aceptar**. Ver la figura 2-9.

Figura 2-9

Permisos efectivos de NTFS



▶ *Copiar y mover archivos*

Cuando se mueven o copian los archivos de una ubicación a otra, es necesario entender lo que ocurre con los permisos de NTFS asociados con estos archivos.

Al copiar y mover archivos, encontrará uno de los siguientes tres escenarios:

- Si copia un archivo o carpeta, el nuevo archivo o carpeta adquirirá automáticamente los mismos permisos que la unidad o carpeta a donde se está copiando.
- Si un archivo o carpeta se mueve dentro del mismo volumen, conservará los mismos permisos que ya le fueron asignados.
- Si un archivo o carpeta se mueve desde un volumen a otro, ese archivo o carpeta adquirirá automáticamente los permisos de la unidad o carpeta a donde se está copiando.

Propietario de carpeta y archivos

El *propietario* de un objeto controla qué permisos se establecen en el objeto y a quién se conceden los permisos. Si por alguna razón, se les ha negado el acceso a un archivo o carpeta y necesitan restablecer los permisos, pueden hacer uso del archivo o carpeta y, a continuación, modificar los permisos. Automáticamente, todos los administradores tienen el permiso de Hacer uso de todos los objetos NTFS.

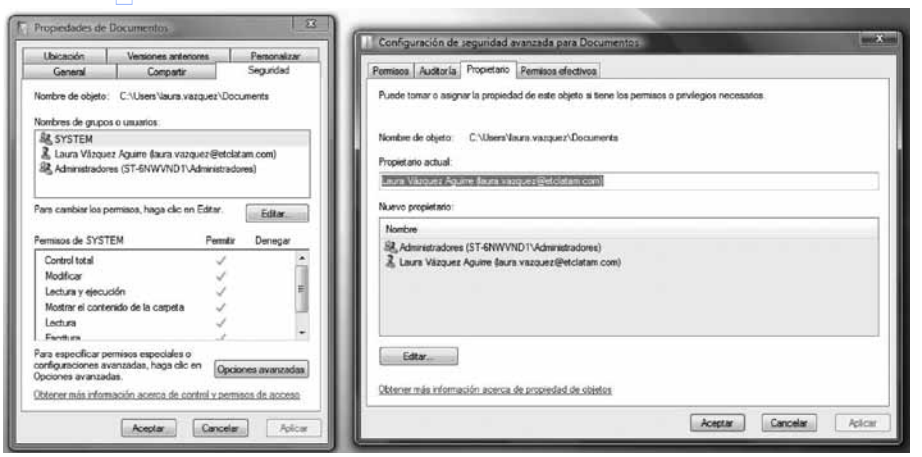
→ Hacer uso de un archivo o carpeta

PREPÁRESE. Para hacer uso de un archivo o carpeta, realice los siguientes pasos:

1. Abra el **Explorador de Windows** y busque el archivo o la carpeta de los que desea hacer uso.
2. Haga clic derecho en el archivo o carpeta, seleccione **Propiedades** y a continuación, elija la pestaña de seguridad.
3. Haga clic en **Propiedades Avanzadas** y posteriormente seleccione la pestaña **Propietario**. Ver la figura 2-10.
4. Haga clic en **Editar** y a continuación realice una de las siguientes acciones:
   - Para cambiar el propietario a un usuario o grupo que no aparece, haga clic en **Otros usuarios y grupos** y en **Escribir el nombre de objeto a seleccionar (ejemplos)**, escriba el nombre de usuario o grupo. Dé clic en **Aceptar**.
   - Para cambiar el propietario a un usuario o grupo que aparece, haga clic en el nombre del nuevo propietario en el cuadro **Cambiar propietario**.
5. Para cambiar el propietario de todos los contenedores secundarios y objetos dentro del árbol, seleccione la casilla de verificación **Reemplazar propietario en subcontenedores y objetos**.

Figura 2-10

Ficha propietario



▪ Hacer uso compartido de unidades y carpetas

↓ EN RESUMEN

La mayoría de los usuarios no van a iniciar una sesión en un servidor directamente para acceder a sus archivos de datos. En su lugar, una unidad o carpeta será compartida (conocida como una ***carpeta compartida***), y accederá a los archivos de datos en la red. Para ayudar a proteger contra el acceso no autorizado a dichas carpetas, va a usar permisos de recurso compartido junto con los de NTFS (suponiendo que la carpeta compartida está en un volumen NTFS). Entonces, cuando los usuarios necesitan tener acceso a un recurso compartido de red, usan la UNC, que es \\nombredelservidor\nombrecompartido.

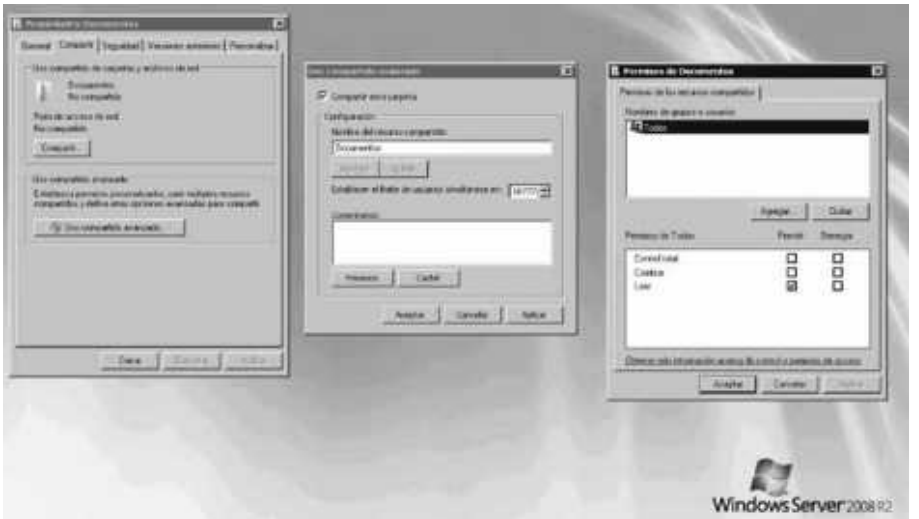
→ Compartir una carpeta

PREPÁRESE. Para compartir una carpeta, sigue estos pasos:

1. En Windows Server 2003, haga clic derecho en la unidad o carpeta que desea compartir y seleccione **Compartir y seguridad**. En Windows Server 2008, haga clic derecho en la unidad o carpeta, seleccione **Propiedades**, seleccione la ficha **Compartir** y a continuación, oprima el botón **Uso compartido avanzado**.
2. Seleccione **Compartir esta carpeta**.
3. Escriba el nombre de la carpeta compartida.
4. Si es necesario, puede especificar el número máximo de personas que pueden tener acceso a la carpeta compartida al mismo tiempo.
5. Haga clic en el botón de **Permisos**.
6. De forma predeterminada, **Todos** reciben el permiso de **Permitir lectura compartida**. A menos que realmente desee que todo el mundo pueda tener acceso a la carpeta, puede quitar **Todos**, asignar permisos adicionales o agregar personas adicionales.
7. Después de que se agregaron a los usuarios y grupos deseados con los permisos adecuados, haga clic en el botón **Aceptar** para cerrar el cuadro de diálogo **Permisos**. Ver la figura 2-11.
8. Haga clic en **Aceptar** para cerrar el cuadro de diálogo **Propiedades**.

Figura 2-11

Compartir una carpeta



Los ***permisos compartidos*** que están disponibles son los siguientes:

- **Control total**: Los usuarios con este permiso tienen permitido Leer y Modificar, así como las capacidades adicionales para cambiar los permisos de archivos y carpetas y tomar propiedad de archivos y carpetas.
- **Cambiar**: Los usuarios tienen permiso de Lectura y capacidades adicionales para crear los archivos y subcarpetas, modificar los archivos, cambiar los atributos de los archivos y subcarpetas y eliminarlos.
- **Lectura**: Los usuarios con este permiso pueden ver nombres de archivos y subcarpetas, acceder a las subcarpetas de los recursos compartidos, leer datos de archivos y atributos y ejecutar archivos de programa.

Cabe señalar que los permisos compartidos siempre aplican cuando se accede de forma remota mediante un UNC, incluso si es en el volumen FAT, FAT32 o NTFS.

Al igual que con NTFS, también puede permitir o denegar el permiso de cada recurso compartido. Para simplificar la administración de los permisos compartidos y NTFS, Microsoft recomienda dar Control total a Todos y a continuación controlar el acceso mediante permisos de NTFS. Además, debido a que un usuario puede ser miembro de varios grupos, es posible que tenga varios conjuntos de permisos en una unidad compartida o carpeta. Los permisos de recursos compartidos eficaces son la combinación de los permisos de usuario y los permisos para todos los grupos de los que el usuario es miembro.

Cuando una persona se registra directamente en la consola del servidor y tiene acceso a los archivos y carpetas sin usar UNC, sólo los permisos de NTFS y (no los permisos compartidos) son aplicables. Por el contrario, cuando una persona tiene acceso a una carpeta compartida utilizando la UNC, debe combinar los permisos compartidos y NTFS para ver qué puede hacer un usuario. Para determinar el acceso general, primero calcule los permisos de NTFS efectivos, luego determine los permisos efectivos compartidos. Por último, aplique los permisos más restrictivos entre ellos.

▶ *Recursos Administrativos Compartidos Especiales*

En Windows, hay varias carpetas compartidas especiales que se crean automáticamente para uso administrativo y del sistema. A diferencia de los recursos regulares, los compartidos no muestran cuando un usuario navega por los recursos de la PC utilizando *Network Neighborhood, My Network Place* o programas de software similares. En la mayoría de los casos, las carpetas compartidas especiales no deberían ser eliminadas o modificadas. Para los servidores de Windows, sólo los miembros del grupo de Administradores, Operadores de las copias de seguridad y Operadores de servidores pueden conectarse a estos recursos.

Un ***recurso administrativo compartido*** es una carpeta compartida que se utiliza normalmente para fines administrativos. Para hacer que una carpeta o unidad compartida sea un recurso compartido oculto, el nombre del recurso compartido debe tener un signo "$" al final del mismo. Debido a que la unidad o carpeta de recurso compartido no se puede ver durante la navegación, tendrá que utilizar un nombre UNC que incluya el nombre del recurso compartido (incluyendo el signo "$"). De forma predeterminada, todos los volúmenes con letras de unidad automáticamente tienen recursos compartidos administrativos (C$, D$, E$, etc.). Según sea necesario para carpetas individuales, se pueden crear otros recursos administrativos compartidos.

Además de los recursos administrativos compartidos para cada unidad, también tendrá los recursos especiales siguientes:

- **ADMIN$**: un recurso utilizado por el sistema durante la administración remota de una PC. La ruta de acceso de este recurso es siempre la ruta de acceso a la raíz del sistema de Windows 7 (el directorio donde está instalado Windows 7, por ejemplo, C:\Windows).
- **IPC$**: un recurso que comparte las canalizaciones con nombre que son esenciales para la comunicación entre programas. Se utiliza durante la administración remota de una PC y cuando se visualizan los recursos compartidos de una PC.
- **PRINT$**: un recurso utilizado durante la administración remota de impresoras.

▪ Introducción al Registro

↓ EN RESUMEN

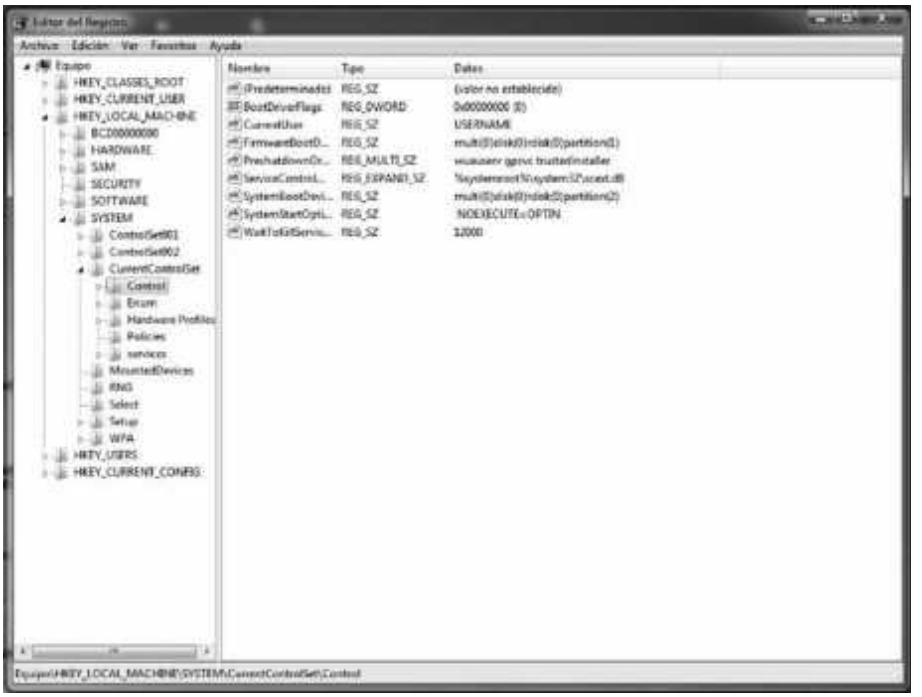
El ***registro*** es una base de datos central y segura en la que Windows almacena toda la información de configuración del hardware, la información de configuración del software y las directivas de seguridad del sistema. Los componentes que utiliza el registro incluyen el núcleo de Windows, los drivers de dispositivos, los programas de instalación, los perfiles de hardware y los perfiles de usuario.

La mayoría de las veces, no necesitará acceder al registro, porque los programas y las aplicaciones normalmente hacen todos los cambios necesarios automáticamente. Por ejemplo, al cambiar el fondo del escritorio o cambiar el color predeterminado para Windows, tiene acceso a la configuración de visualización del Panel de Control y los cambios se guardan automáticamente en el registro.

Si necesita obtener acceso al registro y realizar cambios en él, tiene que seguir puntualmente las instrucciones ofrecidas por una fuente confiable debido a que un cambio incorrecto en el registro de su PC podría hacer que no funcione. Sin embargo, puede presentarse el caso de que tenga que realizar un cambio en el registro, porque no hay interfaz o programa que haga ese cambio. Para ver y cambiar manualmente el registro, se utiliza el Editor del registro (Regedit.exe), el cual se ejecuta desde la línea de comandos, en el cuadro de dialogo de Inicio búsqueda o de Ejecutar. Ver la figura 2-12.

Figura 2-12

Editor del registro



El registro se divide en varias secciones lógicas, que a menudo se denominan "*hives*", y que generalmente son nombrados por sus definiciones de la API de Windows. Los *hives* comienzan con HKEY y son a menudo abreviadas a un nombre corto de tres o cuatro letras, comenzando con "HK." Por ejemplo, HKCU es HKEY_CURRENT_USER, y HKLM es HKEY_LOCAL_MACHINE. Windows 7 tiene cinco claves/HKEYs de raíz:

- **HKEY_CLASSES_ROOT**: Almacena información acerca de las aplicaciones registradas, tal como los datos de asociación de archivos que indica qué programa predeterminado abren los archivos con una cierta extensión.
- **HKEY_CURRENT_USER**: Almacena la configuración específica para el usuario actualmente conectado. Cuando un usuario cierra la sesión, el HKEY_CURRENT_USER se guardará en HKEY_USERS.
- **HKEY_LOCAL_MACHINE**: Almacena la configuración específica para la PC local.
- **HKEY_USERS**: Contiene las subclaves correspondientes a las claves. HKEY_CURRENT_USER para cada perfil de usuario cargado activamente en la PC.
- **HKEY_CURRENT_CONFIG**: Contiene la información recopilada durante el tiempo de ejecución. La información almacenada en esta clave se almacena de forma no permanente en el disco, pero volverá a generarse más bien en el momento del arranque.

Las claves del registro son similares a las carpetas que contienen los valores o las subclaves. Las claves en el registro siguen una sintaxis similar a una carpeta de Windows o a una ruta del archivo que utiliza barras diagonales inversas para separar cada nivel. Por ejemplo:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows

se refiere a la subclave "Windows" de la subclave "Microsoft" de la subclave "Software" de la clave HKEY_LOCAL_MACHINE.

Los valores del registro incluyen un nombre y un valor. Hay varios tipos de valores. Algunos de los tipos más comunes de claves se muestran en el cuadro 2-2.

Cuadro 2-2

Tipos comunes de clave de registro

Nombre	Tipo de datos	Descripción
Valor binario	REG_BINARY	Datos binarios sin formato. La mayor parte de la información sobre componentes de hardware se almacena como datos binarios y se muestra en el Editor de registro en formato hexadecimal.
Valor DWORD	REG_DWORD	Datos representados por un número que tiene cuatro bytes (un entero de 32 bits). Muchos de los parámetros para los drivers de dispositivos y servicios son de este tipo y se muestran en el Editor del registro en formato binario, hexadecimal o decimal.
Valor de cadena expandible	REG_EXPAND_SZ	Una cadena de datos de longitud variable. Este tipo de datos incluye variables que se resuelven cuando un programa o servicio utiliza los datos.
Valor multi-cadena	REG_MULTI_SZ	Una cadena múltiple. Los valores que contienen listas o varios valores en una forma que pueden leer las personas, son generalmente de este tipo. Las entradas están separadas por espacios, comas u otras marcas.
Valor de cadena	REG_SZ	Una cadena de texto de longitud fija.
Valor QWORD	REG_QWORD	Datos representados por un número que es un entero de 64 bits. Esta información se muestra en el Editor del registro como un valor binario y fue introducida en Windows 2000.

Archivos Reg (también conocidos como entradas de registro) son archivos de texto para el almacenamiento de porciones de un registro. Estos archivos tienen una extensión de nombre de archivo. reg. Si hace doble clic en un archivo .reg, agregará las entradas del registro. Puede exportar cualquier subclave del registro haciendo clic derecho en la subclave y seleccionar Exportar. Puede hacer una copia de seguridad de todo el registro a un archivo .reg haciendo clic derecho en Mi PC en la parte superior de Regedit y seleccione Exportar; o puede hacer una copia de seguridad del estado del sistema con Windows Respaldo.

→ Permisos de acceso al registro

PREPÁRESE. El registro utiliza los permisos que se almacenan en Listas de Control de Acceso (ACL). Para acceder a los permisos del registro, realice los pasos siguientes:

1. Abra el **Editor del registro**.
2. Haga clic en la clave a la que desea asignar permisos.
3. En el menú **Edición**, haga clic en **Permisos**.

A continuación, agregará el usuario prospectivo y asignará permisos para Permitir o Denegar Control Total o Lectura.

▪ Hacer uso del encriptado para proteger los datos

↓ EN RESUMEN

Encriptado es el proceso de conversión de datos en un formato que no se puede leer por otro usuario. Una vez que un usuario ha encriptado un archivo, ese archivo automáticamente permanece encriptado cuando se almacena en el disco. ***Desencriptado*** es el proceso de conversión de datos de un formato encriptado a su formato original.

☑ Listo para la Certificación

¿Puede enumerar y contrastar los tres métodos principales de encriptado?
— 2.5

Con el encriptado de uso común, el algoritmo de encriptado debe proporcionar un alto nivel de seguridad estando disponible incluso para el público. Debido a que el algoritmo está a disposición del público, la seguridad reside en la clave, no en el propio algoritmo.

Uno de los algoritmos de encriptado más simples es el encriptado de sustitución, que cambia de un carácter o símbolo a otro. Por ejemplo, si tiene

```
clear text
```

y sustituye cada "e" con una "y," cada "c" con la letra "j" y cada letra "t" con una "y", obtiene el siguiente texto encriptado:

```
jlyar yexy
```

Otra técnica simple se basa en el encriptado de transposición, que implica la transposición o el intercambio de letras de una cierta manera. Por ejemplo, si tiene

```
clear text
```

y se cambia cada dos letras, obtiene:

```
lcae rettx
```

Una ***clave***, que puede considerarse como una contraseña, se aplica matemáticamente a texto sin formato para proporcionar un texto encriptado o codificado. Diferentes claves producen salidas de encriptado diferentes. Con las PC, el encriptado se basa a menudo en bits, no en caracteres. Por ejemplo, si tiene las letras Unicode "cl", se podría expresar en el siguiente formato binario:

```
01100011 01101100
```

Si agregas matemáticamente la forma binaria de ' z'(01111010), que es la clave, se obtiene:

01100011	01101100
+01111010	+ 01111010
11011101	1110 0110

que parecerán caracteres extraños de Unicode:Ýæ.

Al igual que con una contraseña, entre más larga sea la clave (por lo general expresada en bits), es más segura. Para que un hacker averigüe una clave, él o ella también tendrá que utilizar un ataque de fuerza bruta, lo que significa que el hacker tendría que probar todas las combinaciones de bits hasta que él o ella calculen la clave correcta. Aunque una clave podría ser rota si se da el suficiente tiempo y poder de procesamiento, las claves largas son elegidas para que su desencriptado y violación tome meses, incluso años, para lograrse. Por supuesto, al igual que con las contraseñas, algunos algoritmos de encriptado cambian su clave con frecuencia. Por lo tanto, una longitud de clave de 80 bits es generalmente considerada el mínimo para una seguridad fuerte con algoritmos de encriptado simétrico. Las claves de 128 bits se utilizan frecuentemente y también se consideran muy fuertes.

Examen de los tipos de encriptado

Los algoritmos de encriptado se pueden dividir en tres clases: simétrico, asimétrico y de función hash.

Análisis del encriptado simétrico

El encriptado ***simétrico*** utiliza una clave única para encriptar y desencriptar datos. Por lo tanto, también se conoce como clave secreta, clave única, clave compartida y clave privada de encriptado. Para utilizar algoritmos de clave simétrica, es necesario intercambiar inicialmente la clave secreta entre el emisor y el receptor.

El encriptado de claves simétricas puede dividirse en encriptado por bloques y encriptados en flujo. Un encriptado por bloques toma un bloque de texto sin formato y una clave y a continuación, envía un bloque de texto encriptado del mismo tamaño. Dos encriptados de bloque populares son el Estándar de Encriptado de Datos (DES) y el Estándar de Encriptado Avanzada (AES), que han sido designados como estándares de criptografía por el gobierno estadounidense.

La Oficina Nacional de Estándares seleccionó el Estándar de Encriptado de Datos como el estándar de procesamiento de Información Federal oficial (FIPS) para los Estados Unidos en 1976. Se basa en un algoritmo de clave simétrica que utiliza una clave de 56 bits.

Puesto que el DES se basa en un tamaño de clave relativamente pequeño de 56 bits, está sometido a ataques de fuerza bruta. Por lo tanto, en lugar de diseñar un algoritmo de encriptado de bloques completamente nuevo, se desarrolló el Triple DES (3DES), que utiliza tres claves independientes. El DES y el más seguro 3DES son todavía populares y se utilizan en una amplia gama de aplicaciones, que van desde el encriptado de la ATM, a la privacidad del correo electrónico, para asegurar el acceso remoto.

Aunque DES y 3DES siguen siendo populares, un método de encriptado más seguro llamado Estándar de Encriptado Avanzada (AES) fue anunciado en 2001 y actualmente está creciendo en popularidad. Este estándar se compone de tres encriptados de bloque:

AES-128, AES-192 y AES-256 — usado en bloques de 128 bits con tamaños de clave de 128, 192 y 256 bits, respectivamente. Los encriptados AES se han analizado ampliamente y ahora se usan en todo el mundo, incluyendo con el encriptado inalámbrico Wi-Fi de Acceso Protegido 2 (WPA2).

En contraste con el encriptado por bloques, los encriptados en flujo crean una secuencia arbitrariamente larga de material clave, que combina bit a bit o carácter a carácter con el texto sin formato. RC4 es un encriptado de flujo ampliamente utilizado, empleado tanto en Protocolo de Capa de Conexión Segura (SSL) como en WEP (Privacidad Equivalente a Cableado). Aunque RC4 es simple y conocido por su velocidad, puede ser vulnerable si no se descarta la secuencia de clave o si se usan claves no aleatorias o conexas o una única secuencia de clave se utiliza dos veces.

Análisis del encriptado asimétrico

El encriptado ***asimétrico*** también conocido como criptografía de clave pública, utiliza dos claves relacionadas matemáticamente para la codificación. Una de las claves se utiliza para cifrar los datos, mientras que la segunda se utiliza para descifrarla. A diferencia de los algoritmos de clave simétrica, este método no requiere un intercambio inicial seguro de una o más claves secretas para el remitente y el receptor. En su lugar, se puede hacer que la clave pública no sea conocida por nadie y utilizar la otra clave para cifrar o descifrar los datos. La clave pública se puede enviar a alguien o podría publicarse dentro de un certificado digital a través de una autoridad de certificación (AC). Secure Sockets Layer (SSL) / Transport Layer Security (TLS) y Pretty Good Privacy (PGP) utilizan claves asimétricas. Dos protocolos de encriptado asimétrico popular son Diffie-Hellman y RSA.

Por ejemplo, supongamos que desea que un socio le envíe datos. Para iniciar el proceso de encriptado asimétrico, envía a su socio la clave pública. Entonces su socio cifra los datos con la clave y le envía el mensaje encriptado. A continuación usted utiliza la clave privada para desencriptar el mensaje. Si la clave pública cae en manos de otra persona, aún así, esa persona no podrá desencriptar el mensaje porque necesita la clave privada.

Análisis de la función Hash

El último tipo de encriptado es la función hash. A diferencia de los algoritmos simétricos y asimétricos, una ***función hash*** se entiende como un encriptado unidireccional. Eso significa que después de que algo ha sido encriptado con este método, no se puede desencriptar. Por ejemplo, una función de hash puede utilizar para encriptar una contraseña que se almacena en el disco y para firmas digitales. Cada vez que se introduce una contraseña, el mismo cálculo hash se efectúa en la contraseña introducida y en comparación con el valor hash de la contraseña almacenada en el disco. Si los dos coinciden, el usuario debe haber escrito la contraseña. Esto evita almacenar las contraseñas en un formato legible donde un pirata informático podría ser capaz de obtener acceso a ellas.

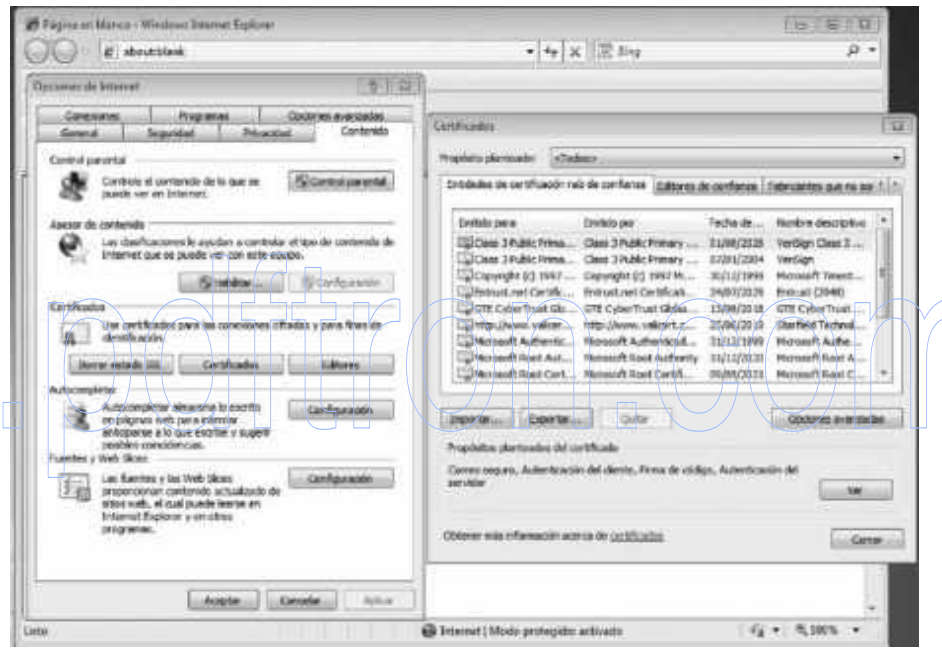
Introducción a la infraestructura de clave pública

Infraestructura de clave pública (PKI) es un sistema que consiste en hardware, software, directivas y procedimientos de creación, administración, distribución, utilización, almacenamiento y revocación de certificados digitales. Dentro de la PKI, la autoridad de certificación (AC) une a una clave pública con las identidades de usuario respectivas y emite los certificados digitales que contienen la clave pública.

Para que el sistema PKI trabaje, la entidad emisora debe ser de confianza. Por lo general dentro de una organización, puede instalar una AC en un servidor Windows, específicamente en un driver de dominio, y sería de confianza dentro de la organización. Si requiere una AC de confianza fuera de la organización, tendría que utilizar una confianza AC de terceros, como VeriSign o Entrust. Las AC establecidas de forma comercial se hacen cargo de emitir certificados en los que se confiará automáticamente por la mayoría de los navegadores web. Ver la figura 2-13.

Figura 2-13

AC de confianza en Internet Explorer



La autoridad de registro (RA), que puede o no ser el mismo servidor que la AC, se utiliza para distribuir las claves, aceptar registros de la entidad emisora y validar identidades. La RA no distribuye certificados digitales; en su lugar, lo hace la AC.

Además de tener una fecha de caducidad, un certificado digital puede ser revocado si se ve comprometido o si la situación ha cambiado para el sistema al que se asignó. Una ***lista de revocación de certificados (CRL)*** es una lista de certificados (o más concretamente, una lista de números de serie para certificados) que han sido revocados o que ya no son válidos y por lo tanto, no se deben utilizar.

Como ya se ha mencionado, los servidores de Windows pueden alojar una autoridad de certificación. La AC raíz de la empresa está en el nivel superior de la jerarquía de autoridad de certificados. Una vez configurada la AC raíz de la empresa, se registra automáticamente dentro del Directorio activo y todos los equipos dentro del dominio confían en ella. Esta autoridad apoyará el registro automático y la opción de renovación automática de los certificados digitales.

Si necesita dar soporte a clientes externos y compradores, probablemente tendría que construir un AC independiente. A diferencia de los AC raíz de empresa, un AC independiente no utiliza el Directorio activo. Porque las AC independientes no admiten registro automático, todas las solicitudes de certificados están pendientes hasta que un administrador las apruebe.

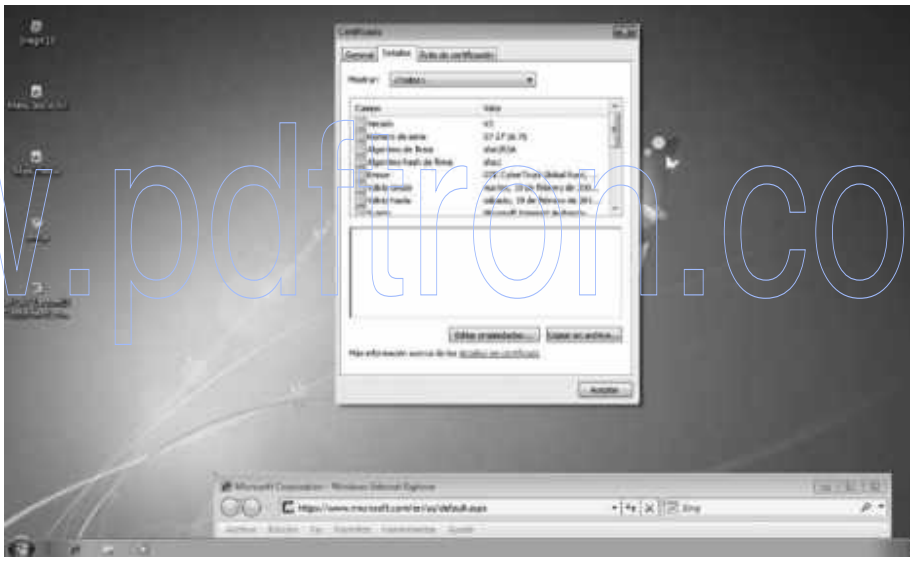
Certificados digitales

Un ***certificado digital*** es un documento electrónico que contiene el nombre de una persona o de la organización, un número de serie, fecha de caducidad, una copia de la clave pública del titular del certificado (utilizado para la encriptación de mensajes y la creación de firmas digitales) y la firma digital de la AC que asigna el certificado para que los destinatarios puedan comprobar que el certificado es real.

El certificado digital más común es el X.509 versión 3. El X.509 versión 3 estándar especifica el formato de certificado de clave pública, listas de revocación de certificados, certificados de atributo y un algoritmo de validación de la ruta de certificado. Ver la figura 2-14.

Figura 2-14

Certificado digital X.509



Los certificados digitales pueden ser importados y exportados a través de archivos electrónicos. Los cuatro formatos más comunes son los siguientes:

- **Intercambio de información personal (PKCS # 12)**: El formato de Intercambio de Información Personal (PFX, también llamado PKCS # 12) admite el almacenamiento seguro de todos los certificados y claves privadas en una ruta de certificación. El formato PKCS # 12 es el único formato de archivo que se puede utilizar para exportar un certificado y su clave privada. Por lo general tendrá una extensión de nombre de archivo .p12.
- **Estándar de Sintaxis de Mensaje Criptográfico (PKCS # 7)**: El formato PKCS # 7 admite el almacenamiento de todos los certificados en una ruta de certificación. Por lo general tendrá una extensión p7b o p7C del nombre de archivo.
- **Certificado codificación binaria DER X.509**: El formato de reglas distinguidas de codificación (DER) admite el almacenamiento de un único certificado. Este formato no es compatible con el almacenamiento de información de la ruta de

certificación o clave privada. Por lo general tendrá una extensión de nombre de archivo .cer, .crt o .der.

- **Codificación Base64 X.509**: El formato Base64 admite el almacenamiento de un único certificado. Este formato no es compatible con el almacenamiento de información de la ruta privada de clave o certificación.

→ Adquirir un Certificado Digital

PREPÁRESE. Para adquirir un certificado digital utilizando IIS 7/7.5, realice los pasos siguientes:

1. Solicite un certificado de servidor de Internet desde el servidor IIS. Para ello, haga clic en el servidor en **Administrador IIS** y posteriormente, doble clic en **Certificados de servidor** en la vista de **Características**. A continuación pulse **Crear una solicitud de certificado** desde el panel de **Acciones**.
2. Envíe la solicitud generada del certificado a la AC, por lo general mediante el sitio Web del proveedor.
3. Reciba un certificado digital de la autoridad de certificación e instálelo en el servidor IIS. De nuevo, abra el **Administrador IIS**, haga doble clic en el servidor en el **administrador IIS** y nuevamente doble clic en **Certificados de servidor** en la vista de **Características**. A continuación, seleccione **Completar solicitud de certificado**.

Si dispone de un centro con varios servidores web, debe instalar el certificado digital del primer servidor y exportarlo a un formato pfx, y tendrá que copiar la clave pública y privada en los otros servidores. Por lo tanto, debe exportar la clave desde el primer servidor e importarla a los otros.

→ Exportar un Certificado Digital

PREPÁRESE. Para exportar un certificado digital, realice los siguientes pasos:

1. Abra **Administrador IIS** y desplácese hasta el nivel que desea administrar.
2. En la vista de **Características**, haga doble clic en **Certificados de servidor**.
3. En el panel de **Acciones**, dé clic en **Exportar**.
4. En el cuadro de diálogo **Exportar**, escriba un nombre de archivo en el cuadro **exportar a** o haga clic en el botón **examinar** para desplazarse hasta el nombre de un archivo y así almacenar el certificado para la exportación.
5. Escriba una contraseña en el cuadro **Contraseña** si desea asociarla con el certificado exportado. Vuelva a escribirla en el cuadro **Confirmar contraseña**.
6. Haga clic en **Aceptar**.

→ Importar un certificado Digital

PREPÁRESE. Para importar un certificado, realice los siguientes pasos:

1. Abra **Administrador IIS** y desplácese hasta el nivel que desea administrar.
2. En la vista de **Características**, haga doble clic en **Certificados de servidor**.
3. En el panel de **Acciones**, haga clic en **Importar**.

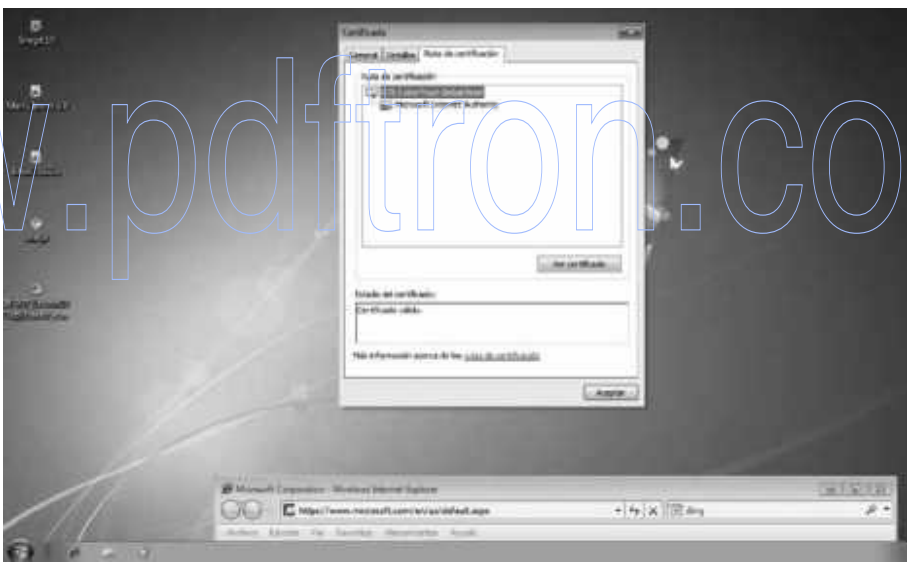
4. En el cuadro de diálogo **Importar Certificado**, escriba un nombre de archivo en el cuadro de **archivo de certificado** o haga clic en el botón **Examinar** para desplazarse hasta el nombre del archivo donde se almacena el certificado exportado. Si el certificado se exportó con una contraseña, escríbala en el cuadro **Contraseña**.
5. Seleccione **Permitir la exportación de este certificado** para poder exportar el certificado, o desactive **Permitir la exportación de este certificado** si desea evitar exportaciones adicionales de este certificado.
6. Haga clic en **Aceptar**.

Examen de una cadena de certificados (Certificate Chain)

Existen solamente tantos certificados de la AC raíz como los que se han asignado a las organizaciones comerciales de terceros. Por lo tanto, al adquirir un certificado digital de una de estas organizaciones, puede ser que necesite usar una cadena de certificados para obtenerlo. Además, puede que deba instalar un certificado digital intermitente que vinculará el certificado digital asignado a un certificado de AC raíz de confianza. La ***cadena de certificados***, también conocida como la ruta de certificado, es una lista de certificados para autenticar una entidad. Comienza con el certificado de la entidad y termina con el certificado de la AC raíz. Ver la figura 2-15

Figura 2-15

Cadena de certificados



Firma Digital

Una ***firma digital*** es un esquema matemático que se utiliza para demostrar la autenticidad de un documento o mensaje digital. Se usa también para demostrar que el mensaje o documento no ha sido modificado. Con una firma digital, el remitente utiliza la clave pública del destinatario para crear un valor hash del mensaje, que se almacena en la síntesis del mensaje. A continuación, se envía el mensaje al receptor. El receptor a continuación utilizará su clave privada para desencriptar el valor hash, realizar la misma función de hash en el mensaje y comparar los valores de dos hash. Si el mensaje no ha cambiado, coincidirá con los valores de hash.

Para demostrar que un mensaje proviene de una persona en particular, puede realizar la función hash con la clave privada y adjuntar el valor hash al documento que se envíe. Cuando el documento es enviado y recibido por la parte receptora, se completa la misma función de hash. A continuación, utilice la clave pública del remitente para desencriptar el valor de hash incluido en el documento. Si coinciden los dos valores de hash, el usuario que ha enviado el documento debe haber sabido la clave privada del remitente, demostrando quién envió el documento. También probará que el documento no ha sido cambiado.

Protocolo de Capa de Conexión Segura (SSL) y Seguridad de la Capa de Transporte (TLS)

Hay veces que se tienen que transmitir datos privados a través de Internet, tales como números de tarjeta de crédito, números de Seguridad Social y así sucesivamente. En estos casos, deberá utilizar SSL sobre http (https) para encriptar los datos antes de enviarlos. Por Convención, las direcciones URL que requieren conexión SSL empiezan con https en lugar de http.

SSL es la abreviatura [en inglés] para ***Protocolo de Capa de Conexión Segura***. Es un sistema criptográfico que utiliza dos claves para encriptar datos, una clave pública conocida por todo el mundo y una clave privada o secreta conocida sólo por el destinatario del mensaje. La clave pública se publica en un certificado digital, que también confirma la identidad del servidor web.

Cuando se conecta a un sitio protegido mediante SSL, aparece un "candado de oro" [*gold lock*] en la barra de direcciones, junto con el nombre de la organización para la cual la AC emitió el certificado. Al hacer clic en el icono del candado, se muestra más información sobre el sitio, incluyendo la identidad de la AC que lo emitió. Si aún así requiere averiguar más sobre el sitio, puede hacer clic en el vínculo Ver certificado para abrir el cuadro de diálogo correspondiente.

Esporádicamente, Internet Explorer puede encontrar problemas con el certificado digital de un sitio Web, por ejemplo, puede estar vencido, puede estar dañado, haber sido revocado o no coincidir con el nombre de la página Web. Cuando esto sucede, IE bloquea el acceso al sitio y muestra un aviso que indica que hay un problema con el certificado. Tendrá una oportunidad de cerrar la ventana del explorador o ignorar la advertencia y continuar hacia el sitio. Por supuesto, si ha optado por ignorar la advertencia, asegúrese de confiar en el sitio Web y de que lo está comunicando con el servidor correcto.

La Seguridad de la Capa de Transporte (TLS) es una extensión del SSL que fue apoyada por Internet Engineering Task Force (IETF) para que pudiera ser un estándar abierto, admitido por la comunidad que, a continuación, podría ampliarse con otros estándares de Internet. Aunque la TLS a menudo se conoce como SSL 3.0, no interactúa con SSL. Además, a pesar de que la TLS es generalmente el valor predeterminado para la mayoría de los navegadores, tiene una función de descenso de categoría que permite al SSL 3.0 ejecutarse según sea necesario.

Codificar el Correo Electrónico

Como el correo electrónico se envía a través de Internet, puede ser que le inquiete la posibilidad de que sus paquetes de datos sean capturados y leídos por otras personas a quienes no van destinados. Por lo tanto, puede que desee encriptar mensajes de correo electrónico que contienen información confidencial.

Hay varios protocolos que pueden utilizarse para encriptar mensajes de correo electrónico. Dos prominentes protocolos incluyen:

- Extensiones de Correo de Internet de Propósitos Múltiples / Seguro (S/MIME)
- Privacidad Bastante Buena (PGP)

S/MIME (Secure Multipurpose Internet Mail Extension) es la versión segura de MIME, utilizada para incrustar objetos dentro de los mensajes de correo electrónico. Es el estándar admitido más ampliamente utilizado para proteger las comunicaciones de correo electrónico, y utiliza el estándar PKCS # 7. S/MIME se incluye con los navegadores web populares y también ha sido respaldada por otros proveedores de productos de mensajería.

PGP (Pretty Good Privacy) es un sistema de encriptado de correo electrónico de software gratuito que utiliza el encriptado simétrico y asimétrico. Aquí, cuando se envía correo electrónico, el documento se encripta con la clave pública y también una clave de sesión. La clave de sesión es un número aleatorio de un solo uso utilizado para crear el texto encriptado. La clave de sesión se encripta en la clave pública y es enviada con el texto encriptado. Cuando se recibe el mensaje, la clave privada se utiliza para extraer la clave de sesión. La clave de sesión y la clave privada se utilizan para desencriptar el texto encriptado.

Encriptar archivos con EFS

Si alguien roba un disco duro que esté protegido por permisos de NTFS, esa persona podría tomarlo y ponerlo en un sistema del que él o ella es administrador y así acceder a todos los archivos y carpetas que se encuentran en éste. Por lo tanto, para proteger verdaderamente una unidad que puede ser robada o a la que se puede acceder ilegalmente, se pueden encriptar los archivos y carpetas en esa unidad.

Windows 7 ofrece dos tecnologías de encriptado de archivos, Sistema de Encriptado de Archivos (EFS) y el encriptado de unidad BitLocker. El EFS protege archivos individuales o carpetas, mientras que BitLocker protege unidades completas.

El Sistema de Encriptado de Archivos (EFS) puede cifrarlos en un volumen NTFS para que no se puedan utilizar a menos que el usuario tenga acceso a las claves necesarias para desencriptar la información. No es necesario que se decodifique antes de poderlo utilizar, más bien, una vez que se encripta un archivo o carpeta, se trabaja con ella tal como se haría con cualquier otra.

El EFS está ajustado a una cuenta de usuario específico, utilizando las claves públicas y privadas que son la base de la infraestructura de clave pública (PKI) Windows. El usuario que crea un archivo es la única persona que puede leerlo. Mientras el usuario trabaja, el EFS encripta los archivos que él o ella crean utilizando una clave generada desde la clave pública del usuario. Pueden desencriptar datos con esta clave sólo por el certificado de encriptado personal del usuario, que se genera utilizando su clave privada.

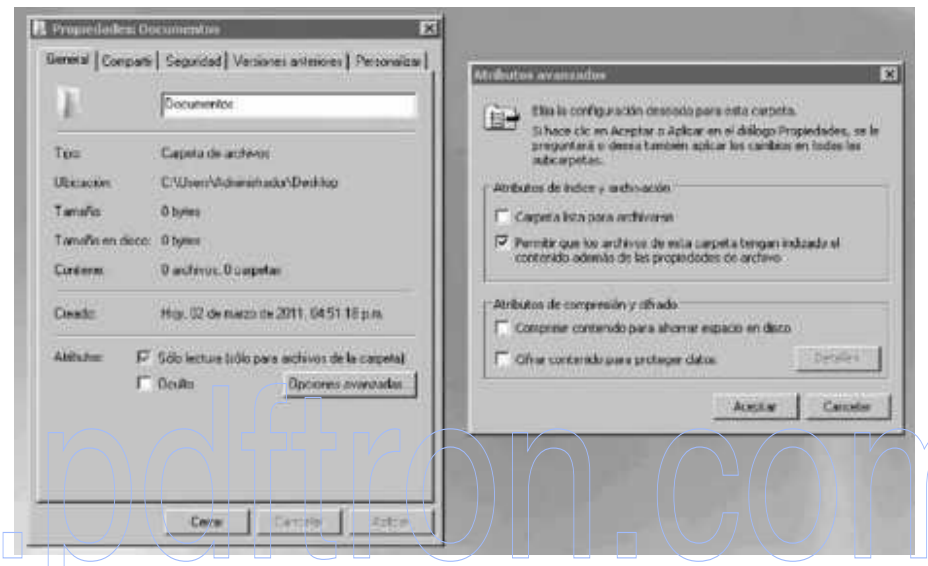
→ Encriptar una carpeta o archivo con EFS

PREPÁRESE. Para encriptar un archivo o carpeta, realice los pasos siguientes:

1. Haga clic derecho en la carpeta o archivo que desee encriptar y a continuación seleccione **Propiedades**.
2. Haga clic en la ficha **General** y a continuación en **Avanzadas**.
3. Seleccione la casilla de verificación **Cifrar contenido para proteger datos**, haga clic en **Aceptar** y posteriormente en **Aceptar**. Ver la figura 2-16.

Figura 2-16

Encriptado de datos con EFS



→ Desencriptar un archivo o carpeta

★ Tome nota

No puede encriptar un archivo con EFS mientras comprime un archivo con NTFS. Sólo se puede hacer una cosa o la otra

PREPÁRESE. Para desencriptar un archivo o carpeta, realice los siguientes pasos:

4. 1. Haga clic derecho en la carpeta o el archivo que desea desencriptar y a continuación en **Propiedades**.
5. 2. Haga clic en la ficha **General** y, a continuación, haga clic en **Avanzadas**.
6. 3. Desactive la casilla de verificación **Cifrar contenido para proteger datos**, haga clic en **Aceptar** y finalmente en **Aceptar**.

La primera vez que encripte una carpeta o archivo, se crea automáticamente un certificado de encriptado. Si el certificado y la clave resultaran perdidos o dañados y no tiene una copia de seguridad, no podrá utilizar los archivos que han sido encriptados. Por lo tanto, debe hacer una copia de seguridad de su certificado de encriptado.

→ Hacer una copia de seguridad del Certificado EFS

PREPÁRESE. Para hacer copia de su certificado de EFS, realice los pasos siguientes:

1. Ejecute **certmgr.msc**. Si se le solicita una contraseña de administrador o la confirmación, escriba la contraseña o proporcione una confirmación.
2. En el panel izquierdo, haga doble clic en **Personal**.
3. Haga clic en **Certificados**.
4. En el panel principal, haga clic en el certificado que muestra el **Sistema de Archivos Encriptados Intencionalmente**. Si hay más de un certificado de EFS, deberá hacer una copia de seguridad de todos ellos.
5. Haga clic en el menú **Acción**, seleccione **Todas las tareas** y posteriormente en **Exportar**.
6. En el Asistente de **Certificado de exportación**, haga clic en **Siguiente**, seleccione **Sí, exportar la clave privada** y después elija **Siguiente**.
7. Haga clic en **Intercambio de información Personal** y a continuación en **Siguiente**.
8. Escriba la contraseña que desea utilizar, confírmela y haga clic en **Siguiente**. El proceso de exportación creará un archivo para almacenar el certificado.
9. Escriba un nombre para el archivo y la ubicación (incluya la ruta de acceso completa) o en su lugar haga clic en **Examinar**, desplácese a una ubicación, escriba un nombre de archivo y haga clic en **Guardar**.
10. Haga clic en **siguiente** y después en **Finalizar**.

A continuación, se debe colocar el certificado en un lugar seguro.

Si por alguna razón, una persona sale de la organización y no puede leer sus archivos encriptados, también puede configurar agentes de recuperación que pueden recuperar los archivos encriptados para un dominio.

→ Agregar usuarios como agentes de recuperación

PREPÁRESE. Para agregar nuevos usuarios como agentes de recuperación, estos usuarios deben tener certificados de recuperación emitidos por la estructura de la autoridad de certificación de empresa.

1. Abra la consola **Administración de directivas de Grupo**.
2. Seleccione la **Default Domain Policy** y haga clic en **Editar**.
3. Expanda Configuración del Equipo, en **Directivas seleccione Configuración de Windows**, después en **Configuración de Seguridad** dé clic en **Directivas de Clave Pública** y finalmente en **Agentes de Recuperación de Datos Encriptados**.
4. Haga clic derecho en **Sistema de cifrado de archivos (EFS)** y seleccione **Agregar agente de recuperación**.
5. Haga clic en **Siguiente para el Asistente de agregar agente de recuperación**.
6. Haga clic en **Examinar el directorio**. Localice el usuario y haga clic en **Aceptar**.
7. Haga clic en **Siguiente**...
8. Haga clic en **Finalizar**...

9. Cierre el **Editor de directivas de grupo**.

Si copia un archivo o carpeta, este adquirirá automáticamente el atributo de encriptado de la carpeta o unidad original. Si el archivo o carpeta se mueve dentro del mismo volumen, conserva el atributo de encriptado asignado originalmente. Por lo tanto, si está encriptado, permanecerá así en la nueva ubicación. Cuando el archivo o carpeta se mueve desde un volumen a otro, es copiado a la nueva ubicación y posteriormente se elimina de la ubicación anterior. Por lo tanto, los archivos y carpetas que se han movido son nuevos en el volumen y adquieren el nuevo atributo de encriptado.

▶ *Encriptar discos de Windows*

A diferencia de EFS, BitLocker permite encriptar discos completos. Por lo tanto, si una unidad o una computadora portátil es robada, los datos estarán todavía encriptados, aún si el ladrón instala otro sistema, del que él o ella es un administrador.

★ Tome nota

BitLocker es una característica de Windows 7 Enterprise y Windows 7 Ultimate. No es compatible con otras ediciones de Windows 7

El encriptado de unidad BitLocker es la característica en las ediciones de Windows 7 Ultimate y Enterprise que hace uso de un Módulo de Plataforma Segura (TPM) del PC. Un TPM es un microchip integrado en una PC que se utiliza para almacenar información criptográfica, tal como las claves de encriptado. La información almacenada en el TPM puede ser más segura frente a ataques de software externo y robo físico. Por ejemplo, el encriptado de unidad BitLocker puede utilizar un TPM para validar la integridad del administrador de arranque de una PC e iniciar los archivos en el arranque, así como garantizar que el disco duro de una PC no haya sido alterado mientras el sistema operativo estaba fuera de línea. El encriptado de unidad BitLocker también almacena mediciones de archivos del sistema operativo central en el TPM.

Los requisitos del sistema de BitLocker son los siguientes:

- Como BitLocker almacena su propia clave de encriptado y desencriptado en un dispositivo de hardware que es independiente del disco duro, debe tener uno de los siguientes:
  - Una PC con el módulo de plataforma segura (TPM). Si su PC fue fabricada con TPM versión 1.2 o posterior, BitLocker almacena su clave en el TPM.
  - Dispositivo extraíble de memoria USB, como una unidad de *USB flash*. Si la PC no tiene versión 1.2 o posterior de TPM, BitLocker almacenará su clave en la unidad flash.
- El equipo también debe tener al menos dos particiones: una partición del sistema (que contiene los archivos necesarios para iniciar la PC y debe ser de al menos 200 MB) y una partición de sistema operativo (que contiene Windows). Se encriptará la partición de sistema operativo, y la partición del sistema se mantendrá sin encriptar por lo que se puede iniciar la PC. Si la PC no tiene dos particiones, Bitlocker las creará. Ambas deben estar formateadas con el sistema de archivo NTFS.
- Además, la PC debe tener un BIOS que es compatible con TPM y admite dispositivos USB durante el inicio de la PC. Si no es el caso, se debe actualizar el BIOS antes de usar BitLocker.

BitLocker tiene cinco modos de funcionamiento, que definen los pasos implicados en el proceso de arranque del sistema. Estos modos, en orden descendente de más a menos seguros, son los siguientes:

- **TPM + NIP de inicio + clave de inicio**: El sistema almacena la clave de encriptado de volumen de BitLocker en el chip TPM, pero un administrador debe proporcionar un número de identificación personal (NIP) e insertar una unidad flash USB que contiene una clave de inicio antes de que el sistema pueda desbloquear el volumen de BitLocker y completar la secuencia de arranque.

- **TPM + clave de inicio**: El sistema almacena la clave de encriptado del volumen de BitLocker en el chip TPM, pero un administrador debe insertar una unidad flash USB que contiene una clave de inicio antes de que el sistema pueda desbloquear el volumen de BitLocker y completar la secuencia de arranque.
- **TPM + NIP de inicio**: El sistema almacena la clave de encriptado del volumen de BitLocker en el chip TPM, pero un administrador debe proporcionar un NIP antes de que el sistema pueda desbloquear el volumen de BitLocker y completar la secuencia de arranque.
- **Clave de inicio únicamente**: El proceso de configuración de BitLocker almacena una clave de inicio en una unidad flash USB, que el administrador debe insertar cada vez que se arranca el sistema. Este modo no requiere que el servidor tenga un chip TPM, pero debe tener un BIOS que admite el acceso a la unidad flash USB antes de la carga del sistema operativo.
- **TPM únicamente**: El sistema almacena la clave de encriptado del volumen de BitLocker en el chip TPM y tiene acceso a esta clave automáticamente cuando el chip ha determinado que el entorno de arranque no ha sido modificado. Esto desbloquea el volumen protegido y la PC continúa con el arranque. Por lo tanto, la intervención administrativa no es necesaria durante la secuencia de arranque.

Cuando se habilita BitLocker mediante el panel de control de Encriptado de Unidad BitLocker, se pueden seleccionar las opciones TPM + clave de inicio, TPM + NIP de inicio o TPM únicamente. Para utilizar el TPM + NIP de inicio + opción clave de inicio, primero se debe configurar la Directiva de grupo *Solicitar autenticación adicional al iniciar*, que se encuentra dentro el contenedor de Configuración de la PC, después en Directivas, ya en este lugar seleccione Plantillas Administrativas y Componentes de Windows. Después en Encriptado de Unidad BitLocker haga clic en Unidades del Sistema Operativo.

Habilitar BitLocker

BitLocker no está habilitado de forma predeterminada. Si no sabe si su computadora portátil viene con TPM, primero debe comprobar que dispone de TPM. A continuación, se encenderá BitLocker para el volumen que desee encriptar.

→ Determinar si la PC tiene TPM

PREPÁRESE. Para saber si su PC dispone de hardware de seguridad del Módulo de Plataforma Segura (TPM), realice los pasos siguientes:

1. Abra el **Panel de Control**, haga clic en **Sistema y Seguridad** y después oprima **Cifrado de Unidad BitLocker**.
2. En el panel izquierdo, haga clic en **Administración de TPM**. Si se le solicita una contraseña de administrador o la confirmación, escriba la contraseña o proporcione una confirmación.

La administración de TPM incorporada en la PC Local indica si la PC tiene el hardware de seguridad TPM. Ver la figura 2-17. Si la PC no lo tiene, se necesitará un dispositivo de memoria USB extraíble para activar BitLocker y almacenar la clave de

Figura 2-17

Consola de administración de TMP

→ Activar BitLocker

PREPÁRESE. Inicie sesión en Windows 7 utilizando una cuenta con privilegios administrativos. A continuación, realice los pasos siguientes:

1. Haga clic en **Inicio** y a continuación haga en **Panel de Control** elija **Sistema y Seguridad**, posteriormente **Cifrado de unidad BitLocker**. Aparecerá el panel de control de encriptado de unidad BitLocker.
2. Haga clic en **Activar BitLocker** para las unidades de disco duro. Aparecerá la página de Preferencias de inicio para establecer BitLocker. Ver la figura 2-18.

Figura 2-18

Activación de BitLocker

3. Haga clic en **Solicitar una clave de inicio al iniciar**. Aparece una página de *Guardar la clave de inicio*.
4. Inserte una unidad flash USB en un puerto USB y haga clic en **Guardar**. Aparecerá la página *¿cómo desea almacenar la clave de recuperación?*
5. Seleccione una de las opciones para guardar la clave de recuperación y haga clic en **Siguiente**. Aparecerá la página *¿está preparado para cifrar esta unidad?*
6. Haga clic en **Continuar**. El asistente realiza una comprobación del sistema y, a continuación reinicie la PC.
7. Inicie sesión en la PC. Windows 7 procederá a encriptar el disco.

Más información

Si la PC tiene un chip TPM, Windows 7 proporciona una consola de administración de Módulo de Plataforma Segura (TPM) que se puede utilizar para cambiar la contraseña del chip y modificar sus propiedades.

Una vez completado el proceso de encriptado, puede abrir el panel de control del cifrado de unidad BitLocker para asegurarse de que el volumen está encriptado o desactivar BitLocker cuando se realice una actualización del BIOS u otro mantenimiento del sistema.

El subprograma del panel de control BitLocker permite recuperar la clave de cifrado y la contraseña a voluntad. Debe considerarse cuidadosamente cómo almacenar esta información, ya que permitirá el acceso a los datos encriptados. También es posible custodiar esta información en el Directorio activo.

BitLocker y agentes de recuperación de datos

Si por alguna razón, un usuario pierde la clave de inicio y/o el NIP necesario para arrancar un sistema con BitLocker, el usuario puede proporcionar la clave de recuperación creada durante el proceso de configuración de BitLocker y obtener acceso al sistema. Sin embargo, si el usuario pierde la clave de recuperación, puede utilizar un agente de recuperación de datos designado con el Directorio activo para recuperar los datos de la unidad.

Un agente de recuperación de datos (DRA) es una cuenta de usuario que un administrador ha autorizado para recuperar unidades de BitLocker para toda una organización con un certificado digital en una tarjeta inteligente. En la mayoría de los casos, los administradores de redes de servicios de dominio de Directorio activo (AD DS) utilizan DRA para garantizar el acceso a sus sistemas protegidos mediante BitLocker y para evitar tener que mantener el gran número de claves individuales y NIP.

Para crear un DRA, primero debe agregar la cuenta de usuario que desee designar para el contenedor de Configuración de la PC\Configuración de Windows\Configuración de Seguridad\Directivas de Clave Pública\Encriptado de Unidad BitLocker en un GPO o para la Directiva de Seguridad Local del sistema. A continuación, se debe configurar la configuración de la directiva de Proporcionar Identificadores Únicos de su Organización en el contenedor de Configuración de la PC\Directivas\Plantillas Administrativas\Componentes de Windows\Encriptado de Unidad BitLocker con campos únicos de identificación para la unidad BitLocker.

Por último, se debe habilitar la recuperación por el DRA para cada tipo de recurso de BitLocker que se desea recuperar mediante la configuración de las directivas siguientes:

- Elegir cómo pueden ser recuperadas las unidades de sistema operativo protegidas mediante BitLocker
- Elegir cómo pueden ser recuperadas las unidades de disco duro fijas protegidas mediante BitLocker
- Elegir cómo pueden ser recuperadas las unidades de disco extraíbles protegidas mediante BitLocker

Estas directivas permiten especificar cómo los sistemas BitLocker deben almacenar la información de recuperación, y también permiten almacenar esa información en la base de datos de AD DS.

BitLocker To Go

BitLocker To Go es una nueva característica de Windows 7 que permite a los usuarios encriptar los dispositivos USB extraíbles, como unidades flash y discos duros externos. Aunque BitLocker siempre ha apoyado el encriptado de unidades extraíbles, BitLocker To Go permite usar el dispositivo encriptado en otros equipos sin tener que realizar un proceso de recuperación involucrado. Debido a que el sistema no es utilizando en la unidad extraíble como dispositivo de arranque, no se requiere un chip TPM.

Para utilizar BitLocker To Go, inserte la unidad extraíble y abra el panel de control de encriptado de unidad BitLocker. El dispositivo aparece en la interfaz, con un vínculo *activar BitLocker* al igual al de la unidad de disco duro de la PC.

▪ Introducción a IPsec

↓ **EN RESUMEN**

Seguridad del protocolo Internet, más conocida como ***IPsec***, es un conjunto de protocolos que proporciona un mecanismo para la integridad de los datos, autenticación y privacidad para el Protocolo de Internet. Se usa para proteger los datos que se envían entre host en una red mediante la creación de túneles electrónicos seguros entre dos máquinas o dispositivos. IPsec se puede utilizar para acceso remoto, VPN, conexiones del servidor, conexiones LAN o conexiones WAN.

IPsec garantiza que los datos no se pueden ver o modificar por usuarios no autorizados, mientras que se están enviando a su destino. Antes de que los datos se envíen entre dos host, la PC de origen encripta la información mediante el encapsulamiento de cada paquete de datos en un nuevo paquete que contiene la información necesaria para configurar, mantener y derribar el túnel cuando ya no es necesario. Los datos se desencriptan, a continuación, en la PC de destino.

Hay un par de modos y un par de protocolos disponibles en IPsec dependiendo de si son implementados por los host finales (por ejemplo, el servidor) o implementados en los routers y el nivel de seguridad deseado. En particular, IPsec se puede utilizar en uno de dos modos:

- **El modo de transporte**: Utilizado para comunicaciones seguras end-to-end, como entre un cliente y un servidor.
- **Modo de túnel**: Utilizado para configuraciones de servidor a servidor o servidor de gateway. El túnel es la ruta que un paquete toma desde la PC de origen hasta la PC de destino. De esta forma, todos los paquetes IP enviados entre los dos equipos o entre las dos subredes, dependiendo de la configuración, están asegurados.

Además, los dos protocolos IPsec son los siguientes:

- **Encapsulating Security Payload (ESP)**: Proporciona confidencialidad, autenticación, integridad y protección contra réplica únicamente para la carga IP, no para todo el paquete. ESP opera directamente en la parte superior del IP.

- **Authentication Header (AH):** Proporciona autenticación, integridad y protección contra réplica para todo el paquete (tanto para el encabezado IP como para la carga de datos transportados en el paquete). No proporciona confidencialidad, lo cual significa que no encripta la carga. Los datos son legibles pero están protegidos contra modificaciones. Algunos campos que están permitidos de modificar durante el tránsito están excluidos porque necesitan ser modificados en la medida en que se transmiten de un router a otro. AH opera directamente en la parte superior del IP.

Estos protocolos pueden combinarse para proporcionar autenticación, integridad y protección contra réplica para todo el paquete (el encabezado IP y la carga de datos en el paquete), así como la confidencialidad de la carga útil.

Aunque AH y ESP proporcionan los medios para proteger los datos de las manipulaciones, prevenir intrusos y verificar el origen de los datos, es el Intercambio de Claves de Internet (IKE) el que define el método para el intercambio seguro de las claves de encriptado inicial entre los dos puntos de comunicación. Además permite que los nodos concuerden en cuanto a los métodos de autenticación, métodos de encriptado, qué claves usar y la vida útil de las claves.

La información negociada por IKE se almacena en una asociación de seguridad (SA), que es como un contrato en el que se establecen las normas de la conexión VPN para la duración. A cada SA es asignado un número de 32 bits que, cuando se utiliza junto con la dirección IP de destino, identifica de forma única la SA. Este número se llama el índice de parámetros de seguridad (SPI).

IPsec se puede utilizar con Windows de varias maneras. Para habilitar a las comunicaciones de IPsec en una PC Windows Server 2008, se deberán crear directivas de grupo y asignarlas a los equipos individuales o grupos de equipos. También se puede utilizar el firewall de Windows con seguridad avanzada.

▶ Encriptado con tecnología VPN

Hoy en día, es común para las organizaciones utilizar servidores de acceso remoto (RAS), que permite a los usuarios conectarse remotamente a través de diversos protocolos y tipos de conexión. Al conectarse a RAS por Internet, los usuarios pueden conectarse a la red de su organización para acceder a los archivos de datos, leer el correo electrónico y acceder a otras aplicaciones como si estuvieran en el trabajo. Sin embargo, debido a que Internet se considera un medio no seguro, se debe utilizar el encriptado de datos al configurar estos tipos de conexiones.

Una ***red privada virtual (VPN)*** une dos equipos a través de una red de área amplia, como Internet. Para mantener la conexión segura, los datos enviados son encapsulados y encriptados. En un escenario, un cliente se conecta al servidor RAS para tener acceso a recursos internos desde fuera del sitio. Otro escenario es conectar un servidor RAS en un sitio u organización a otro servidor RAS en otro sitio u organización para que los sitios o las organizaciones puedan comunicarse entre sí.

Los tres tipos de protocolos de túnel que se utilizan con un servidor VPN/ servidor/RAS que se ejecutan en Windows Server 2008 R2 son los siguientes:

- **Point to Point Tunneling Protocol (PPTP)**: Protocolo VPN basado en el Protocolo de punto a punto heredado utilizado con los módems. Por desgracia, PPTP es fácil de configurar pero utiliza tecnología de encriptado débil.
- **Layer 2 Tunneling Protocol (L2TP)**: Se utiliza con IPsec para proporcionar seguridad. Este es el estándar de la industria al configurar túneles seguros.
- **Secure Sockets Tunneling Protocol (SSTP)**: Introducido con Windows Server 2008, que usa el Protocolo HTTPS sobre el TCP puerto 443 para pasar el tráfico a

través de firewall y servidores proxy de web que podrían bloquear PPTP y L2TP/IPsec.

- **Internet Key Exchange2 (IKEv2)**: Utiliza IPsec para el encriptado y soporta VPN para volver a conectar (también llamada Movilidad), que permite a las conexiones de VPN mantenerse cuando un cliente VPN se mueve entre celdas inalámbricas o conmutadores y automáticamente restablece la conectividad VPN rota. A diferencia de L2TP con IPsec, los equipos cliente de IKEv2 no necesitan proporcionar autenticación a través de un certificado de equipo o una clave previamente compartida.

Al utilizar VPN, Windows 7 y Windows Server 2008 soportará las siguientes formas de autenticación:

- **Password Authentication Protocol (PAP)**: Utiliza texto sin formato (contraseñas sin encriptar). PAP es la forma menos segura de autenticación y no se recomienda.
- **Challenge Handshake Authentication Protocol (CHAP)**: Un método de autenticación de desafío y respuesta que utiliza el esquema de hashing md5, estándar de la industria, para encriptar la respuesta. CHAP fue un estándar de industria durante años y sigue siendo muy popular.
- **Microsoft CHAP versión 2 (MS-CHAP v2)**: Proporciona autenticación de dos vías (autenticación mutua). MS-CHAP v2 proporciona una mayor seguridad que CHAP.
- **Extensible Authentication Protocol Microsoft CHAP version 2 (EAP-MS-CHAPv2)**: EAP es un marco de autenticación universal que permite a los proveedores de terceros desarrollar esquemas de autenticación personalizados incluyendo análisis de retina, reconocimiento de voz, identificaciones de huellas digitales, tarjetas inteligentes, Kerberos y certificados digitales. También proporciona un método de autenticación mutua que soporta la autenticación basada en contraseñas de usuario o equipo.

→ Crear un túnel VPN

PREPÁRESE. Para crear un túnel VPN en una PC que ejecuta Windows 7 para conectarse a un servidor de acceso remoto, siga estos pasos:

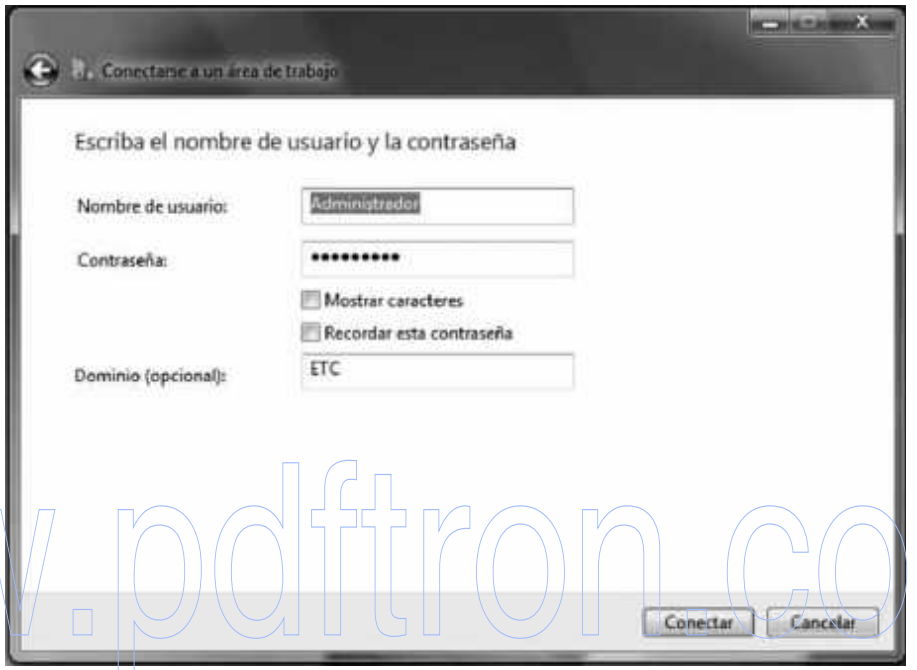
1. Desde el **Panel de Control**, seleccione **Red e Internet** para acceder a la **Red y al Centro de recursos compartidos**.
2. En **Red y Centro de recursos compartidos** elija configurar un A**sistente para conexión nueva**.
3. En la página **Configurar una conexión o red**, seleccione **Conectarse a un lugar de trabajo**.
4. En la página **Conectar con un lugar de trabajo**, responder a la pregunta: **¿desea utilizar una conexión que ya tiene?** Elija si desea crear una nueva conexión o utilizar una conexión existente.
5. En la siguiente página, elija **Usar mi conexión a Internet (VPN)**.
6. En la siguiente pantalla, elija su conexión VPN o especifique la dirección de Internet para el servidor VPN y un nombre de destino. También puede especificar las siguientes opciones: **Utilizar una tarjeta inteligente para la autenticación**, **Permitir que otras personas usen esta conexión** y **No conectar ahora, sólo instalar para que pueda conectarme más tarde**.

A menudo, puede ser que necesite configuraciones adicionales de su conexión de VPN, tales como las que se especifican el tipo de Protocolo, qué Protocolo de autenticación utilizar y el tipo de encriptado.

Después de crear la conexión VPN y configurarla, para conectar mediante la VPN, simplemente abre el centro de redes y recursos compartidos y haga clic en Administrar Conexiones de Red. A continuación, pulse el botón derecho de su conexión VPN y haga clic en el botón Conectar. Ver la figura 2-19.

Figura 2-19

Conexión VPN



De forma predeterminada, cuando se conecta a una VPN usando la configuración anterior, toda la navegación en web y el tráfico de la red pasa por la puerta de enlace predeterminada en la Red Remota a menos que se esté comunicando con los equipos locales de la casa. Con esta opción activada ayuda a proteger la red corporativa puesto que también todo el tráfico pasará a través de los firewall y servidores proxy, lo cual ayuda a evitar que una red sea infectada o se vea comprometida.

Si desea enrutar su navegación a través de su conexión a Internet personal en vez de a través de la red corporativa, puede deshabilitar la opción de "Usar Gateway Predeterminada en Red Remota". Al desactivar esta opción, está utilizando lo que se conoce como división de túnel.

→ Habilitar la división de túnel

PREPÁRESE. Para habilitar la división de túnel, realice los pasos siguientes:

1. Haga clic derecho en una conexión VPN y haga clic en **Propiedades**.
2. Haga clic en la ficha **Funciones de red**.
3. Haga doble clic en **Protocolo de Internet versión 4 (IPv4)**
4. Haga clic en el botón **Opciones avanzadas**.

5. Desactive la opción de **Usar la puerta de enlace predeterminada en la red remota**.

Puede significar mucho trabajo el configurar varios clientes para conectarse a un servidor de acceso remoto. De hecho, esta tarea es a menudo demasiado complicada para novatos de la computación, y puede prestarse a errores. Para ayudar a simplificar la administración del cliente VPN en un ejecutable fácil de instalar, se puede utilizar el Paquete de Administración del Gestor de Conexión (CMAK). Para instalar CMAK en Windows Server 2008, debe instalarlo como una característica.

▪ Auditoría para Completar el cuadro de Seguridad

↓ EN RESUMEN

Como se mencionó anteriormente, la seguridad puede dividirse en tres áreas. La autenticación se utiliza para probar la identidad de un usuario, mientras que la autorización da acceso a un usuario autenticado. Para completar el cuadro de seguridad, sin embargo, necesita habilitar la auditoría para que usted pueda tener un registro de los usuarios que han iniciado sesión y a qué recursos aquellos usuarios han tenido acceso o han intentado acceder.

☑ Listo para la Certificación

¿Puede explicar por qué la auditoría es tan importante para la seguridad?
— 2.4

Es importante que proteja su información y recursos de servicio contra personas que no deben tener acceso a ellos, mientras que al mismo tiempo esos recursos están a disposición de los usuarios autorizados. Por lo tanto, junto con la autenticación y autorización, también debe habilitarse la auditoría para que pueda tener un registro de los siguientes datos:

- ¿Quién ha iniciado sesión de manera efectiva?
- ¿Quién ha intentado iniciar sesión pero no lo ha logrado?
- ¿Quién ha cambiado las cuentas en el Directorio activo?
- ¿Quién ha accedido o cambiado ciertos archivos?
- ¿Quién ha utilizado una cierta impresora?
- ¿Quién ha reiniciado un sistema?
- ¿Quién ha hecho algunos cambios en el sistema?

La auditoría no está habilitada de forma predeterminada en Windows. Para habilitar la auditoría, debe especificar qué tipos de eventos del sistema serán auditados mediante el uso de directivas de grupo o de la directiva de seguridad local (Configuración de Seguridad después en Directivas Locales y finalmente en Directiva de Auditoría). Ver la figura 2-20. El Cuadro 2-3 muestra los eventos de auditoría básica que están disponibles en Windows Server 2003 y 2008. Windows Server 2008 también tiene opciones adicionales para un control más detallado. Después de habilitar el registro, a continuación, abra los registros de seguridad del Visor de sucesos para ver los eventos de seguridad registrados. De forma predeterminada, estos registros sólo pueden ser vistos y gestionados por el grupo de administradores.

Figura 2-20

Habilitar la auditoría de uso de directivas de grupo

Cuadro 2-3

Eventos de auditoría

Evento	Explicación
Inicio de sesión de cuenta	Determina si el sistema operativo audita cada vez que la PC valida las credenciales de una cuenta, tal como el inicio de sesión de una cuenta.
Administración de cuentas	Determina si se debe auditar cada evento de gestión de la cuenta en una PC, incluyendo el cambio de contraseñas y crear o eliminar cuentas de usuario.
Acceso del servicio de directorio	Determina si el sistema operativo audita los intentos del usuario de acceder a objetos del Directorio activo.
Inicio de sesión	Determina si el sistema operativo audita cada instancia de un usuario que intenta iniciar sesión o cerrar la sesión en su PC.
Acceso a objetos	Determina si el sistema operativo audita los intentos del usuario por tener acceso a objetos que no están en el Directorio activo, incluidos archivos, carpetas e impresoras NTFS.
Cambio de directiva	Determina si el sistema operativo audita cada instancia en la que los usuarios intentan cambiar las asignaciones de derechos de usuario, la Directiva de auditoría, la Directiva de cuentas o directiva de confianza.
Uso de privilegios	Determina si se debe auditar cada instancia en la que un usuario ejerce un derecho de usuario.
Proceso de seguimiento	Determina si el sistema operativo audita los sucesos relacionados con el proceso, tales como el proceso de creación, finalización de los procesos, duplicación de identificadores y acceso de objeto indirecto. Se suele utilizar para solucionar problemas.
Sistema	Determina si el sistema operativo audita cambios en la hora del sistema, inicio o cierre del sistema, intentos de cargar componentes de autenticación extensible, pérdidas de auditoría de eventos debido a fallos en el sistema y registros de seguridad que exceden el nivel de umbral de advertencia que se puede configurar.

La auditoría de archivos NTFS, carpetas e impresoras es un proceso de dos pasos. Primero debe habilitarse el acceso a objetos mediante las directivas de grupo. A continuación, deben especificarse los archivos, carpetas o impresoras que se desee auditar. Después de habilitar el registro, se pueden abrir los registros de seguridad del Visor de sucesos para ver los eventos de seguridad.

Dado que Windows es sólo una parte de lo que forma parte de una red, también se necesita mirar otras áreas para auditar. Por ejemplo, para un servidor de web de Microsoft IIS, puede habilitarse el registro de quién visita cada sitio. Para Microsoft's Internet Security and Acceleration (ISA) y Microsoft's Threat Management (TMG), se puede elegir registrar quién accede a la red a través de una VPN o a lo que se tiene acceso a través del cortafuegos. También, si dispone de servidores de seguridad y routers Cisco, se debe habilitar la auditoría de manera que si alguien reconfigura el router y el servidor de seguridad, se tenga un registro de la misma.

Si necesita auditar productos que no son de Microsoft, puede que necesite utilizar Syslog. ***Syslog*** es un estándar para el registro de mensajes de programa a los que se puede acceder por medio de dispositivos que de lo contrario no tendrían un método para las comunicaciones. Los cortafuegos y routers de Cisco, equipos con Linux y UNIX, y muchas impresoras pueden utilizar Syslog. Puede ser empleado para la administración del sistema de equipos y auditorías de la seguridad, así como para información general, análisis y mensajes de depuración.

Por último, se debe asegurar que dispone de un sistema de administración de cambios y un sistema de pases de entrada. El primero registra qué modificaciones se han hecho. Proporciona un método para revisar los cambios antes de su aplicación para que si estos cambios causan problemas en un sistema, puedan evaluarse por el departamento de TI. Además, si se produce un problema, proporciona una lista de todos los cambios realizados en el entorno.

En comparación, el segundo da un registro de todos los problemas y las peticiones de los usuarios. Al tener un sistema de pases de entrada, se puede determinar cuáles son los problemas más comunes y determinar las tendencias.

→ Utilizar archivos de auditoría y carpetas

PREPÁRESE. Suponiendo que la auditoría de objetos se ha habilitado, para auditar archivos y carpetas, siga estos pasos:

1. Abra el **Explorador de Windows**.
2. Haga clic derecho en el archivo o carpeta que desee auditar, seleccione **Propiedades** y a continuación la ficha **Seguridad**.
3. Haga clic en **Opciones Avanzadas**.
4. En el cuadro de diálogo **Configuración de seguridad avanzada para <objeto>**, haga clic en la ficha **auditoría**.
5. Siga uno de estos procedimientos:
   - Para configurar la auditoría para un nuevo usuario o grupo, haga clic en **Agregar**. En **Escriba el nombre de objeto a seleccionar**, escriba el nombre del usuario o grupo que desee y a continuación oprima **Aceptar**.
   - Para quitar la auditoría de un grupo o un usuario existente, haga clic en el nombre del grupo o el nombre de usuario, seleccione **Quitar**, oprima **Aceptar** y a continuación omita el resto de este procedimiento.

- Para ver o cambiar la auditoría de un grupo o usuario existente, haga clic en el nombre del grupo o usuario y seleccione **Editar**.

6. En el cuadro **Aplicar en**, haga clic en la ubicación donde va a tener lugar la auditoría.
7. En el cuadro de **Acceso**, indique qué acciones desea auditar seleccionando las casillas correspondientes:
   - Para auditar los eventos con éxito, active la casilla de verificación **Correcto**.
   - Para dejar de auditar los eventos con éxito, desactive la casilla de verificación **Correcto**.
   - Para auditar los eventos sin éxito, active la casilla de verificación de **Error**.
   - Para dejar de auditar eventos sin éxito, desactive la casilla de verificación de **error**.
   - Para dejar de auditar todos los eventos, haga clic en **Borrar todo**.
8. Si desea evitar que los siguientes archivos y subcarpetas del objeto original hereden estas entradas de auditoría, active la casilla de verificación **incluir todas las entradas de auditoría heredables del objeto principal a este objeto**.
9. Haga clic en **Aceptar** para cerrar el cuadro de diálogo C**onfiguración de seguridad avanzada**.
10. Haga clic en **Aceptar** para cerrar el cuadro de diálogo **Propiedades**.

Resumen de matriz de habilidades

En esta lección usted aprendió:

- El AAA (Autenticación, Autorización y Auditoría) es un modelo para el control de acceso.
- Autenticación es el proceso de identificación de un individuo.
- Después de que un usuario se autentica, él o ella puede acceder a recursos de red en función de su autorización. La autorización es el proceso de dar a los individuos acceso a objetos del sistema en función de su identidad.
- Las cuentas de usuario, también conocida como auditoría, es el proceso de seguimiento de la actividad de un usuario cuando accede a los recursos de la red, incluida la cantidad de tiempo que pasa en ella, los servicios a los que tiene acceso, y la cantidad de datos transferidos durante la sesión.
- La confirmación de firma impide que una de las partes deniegue las acciones que han llevado a cabo.
- Los usuarios pueden autenticarse utilizando lo que saben, lo que poseen o lo que son.
- Al utilizar dos o más métodos para autenticar un usuario, se está implementando un sistema de autenticación con varios factores.
- La contraseña es el método más común de autenticación en las PC y las redes.
- Una contraseña es una serie secreta de caracteres que permite a un usuario acceder a un archivo, equipo o programa.
- Para violar una contraseña, los piratas tratarán contraseñas obvias, ataques por fuerza bruta y ataques de diccionario.
- Para aumentar la seguridad, se debe elegir una contraseña que nadie pueda adivinar. Por lo tanto, la contraseña debe ser lo suficientemente larga, y se debe considerar fuerte o compleja.
- Un número de identificación personal (NIP) es una contraseña numérica secreta compartida entre un usuario y un sistema que puede ser utilizada para autenticar al usuario en el sistema.

- Un certificado digital es un documento electrónico que contiene una identidad, como un usuario u organización y una clave pública correspondiente.
- Una tarjeta inteligente es una tarjeta de bolsillo con circuitos integrados incrustados, que consisten en componentes de almacenamiento de memoria no volátil y tal vez una lógica de seguridad dedicada.
- Una tarjeta inteligente puede contener certificados digitales para probar la identidad de la persona que porta la tarjeta, y también puede contener permisos y tener acceso a información.
- La biometría es un método de autenticación que identifica y reconoce las personas con base en rasgos físicos, tales como huellas dactilares, reconocimiento facial, reconocimiento del iris, exploraciones de la retina y reconocimiento de voz.
- Puesto que los administradores tienen acceso completo a equipos y redes, debe utilizar una cuenta estándar de no administrador para realizar la mayoría de las tareas.
- Directorio activo es una tecnología creada por Microsoft que ofrece una variedad de servicios de red, incluyendo LDAP, autenticación basada en Kerberos y única de inicio de sesión, asignación de nombres basados en DNS y otra información de la red, y una ubicación central para la administración de la red y delegación de autoridad.
- Kerberos es el Protocolo de autenticación de red de equipo predeterminado. Permite a los host probar su identidad a través de una red no segura en una manera segura.
- El inicio de sesión único (SSO) permite iniciar sesión una vez y acceder a múltiples sistemas de software relacionados, pero independientes, sin tener que iniciar sesión nuevamente.
- Una cuenta de usuario permite a un usuario iniciar sesión en una PC y un dominio.
- Las cuentas de usuario locales se almacenan en la base de datos del administrador de cuentas de seguridad (SAM) en la PC local.
- Los grupos se utilizan para agrupar usuarios y equipos de modo que al asignar derechos y permisos, se pueden asignar a todo el grupo, en lugar de a cada usuario individualmente.
- Un derecho autoriza a un usuario a realizar determinadas acciones en una PC, como el inicio de sesión en un sistema de forma interactiva o copias de seguridad de archivos y directorios en un sistema.
- Un permiso define el tipo de acceso que se concede a un objeto o atributo de objeto.
- Los permisos explícitos son permisos concedidos directamente a un archivo o carpeta.
- Los permisos heredados son permisos que se conceden a una carpeta (objeto primario o contenedor) y, a continuación, desembocan en los objetos de las carpetas secundarias (subcarpetas o archivos dentro de la carpeta principal).
- El propietario de un objeto controla cómo se establecen los permisos en el objeto y a quién se conceden los permisos.
- El encriptado es el proceso de convertir los datos en un formato que no se puede leer por otro. Una vez que un usuario ha encriptado un archivo, este automáticamente permanece encriptado cuando se almacena en el disco.
- El desencriptado es el proceso de conversión de datos desde un formato de encriptado a su formato original.
- Los algoritmos de encriptado se pueden dividir en tres clases: simétricos, asimétricos y de función hash.
- El encriptado simétrico utiliza una clave única para encriptar y desencriptar datos. Por lo tanto, también se conoce como encriptado de clave secreta, clave única, clave compartida y clave privada.

- El encriptado de clave asimétrica, también conocido como la criptografía asimétrica, utiliza dos claves matemáticamente relacionadas. Una de ellas se utiliza para encriptar los datos, mientras que la segunda se utiliza para desencriptarlos.
- Diferentes de los algoritmos simétricos y asimétricos, una función de hash se entiende como un encriptado unidireccional. Eso significa que después de que la información ha sido encriptada, no se puede desencriptar.
- La infraestructura de clave pública (PKI) es un sistema que consiste en hardware, software, directivas y procedimientos de creación, administración, distribución, uso, almacenamiento y revocación de certificados digitales.
- El certificado digital más común es el X.509 versión 3.
- La cadena del certificado, también conocida como la ruta de certificación, es una lista de certificados para autenticar una entidad. Comienza con el certificado de la entidad y finaliza con el certificado de la CA de raíz.
- Una firma digital es un esquema matemático que se utiliza para demostrar la autenticidad de un mensaje digital o documento. También se utiliza para demostrar que no se ha modificado el mensaje o documento.
- Cuando necesite transmitir datos privados a través de Internet, deberá utilizar SSL sobre HTTPS (https) para encriptar los datos que vas a enviar. Las direcciones URL que requieren un inicio de conexión SSL con https en lugar de http.
- La seguridad IP, más conocida como IPsec, es un conjunto de protocolos que proporcionan un mecanismo para la integridad de los datos, la autenticación y para el Protocolo de Internet.
- Una red privada virtual (VPN) enlaza dos equipos a través de una red de área amplia, como Internet.
- Syslog es un estándar para el registro de mensajes de programas a los que se puede acceder por medio de dispositivos que de otra manera no tendrían un método de comunicación.

» Evaluación del conocimiento

Opción múltiple

Encierre en un círculo la letra que corresponda a la mejor respuesta.

1. ¿Cuál de los siguientes no es un método para la autenticación?
   a. Algo que el usuario sabe
   b. Algo de lo que el usuario es propietario o posee
   c. Encriptado
   d. Algo que el usuario es
2. ¿Cuál de los siguientes no es un dispositivo biométrico?
   a. Lector de contraseñas
   b. Escáner de retina
   c. Escáner de huellas digitales
   d. Analizador de cara
3. ¿Cuál de los siguientes servicios se utiliza para la autenticación centralizada, autorización y auditoría?
   a. VPN
   b. PGP

c. c. RADIUS
d. d. PKI

4. ¿Cuál es el método de autenticación principal utilizado en Directorio activo de Microsoft?
   a. LDAP
   b. Kerberos
   c. NTLAN
   d. SSO
5. 5. El guardián maestro del tiempo y maestro para los cambios de contraseña en un dominio de Directorio activo es el:
   a. Emulador de PDC
   b. RID
   c. Maestro de infraestructuras
   d. Maestro de esquema
6. Las cuentas de usuario locales se encuentran en:
   a. Directorio activo
   b. Registro
   c. SAM
   d. LDAP
7. Un _____ autoriza a un usuario para realizar determinadas acciones en una PC
   a. Permiso
   b. Algoritmo de encriptado
   c. Protocolo de autenticación
   d. Derecho

8. ¿Cuál de los siguientes sistemas de archivo ofrece la mejor seguridad?
   a. FAT
   b. FAT32
   c. NTFS
   d. EFS
9. 9. ¿Qué permiso NTFS es necesario para cambiar los atributos y permisos?
   a. Control total
   b. Modificar
   c. Lectura y Ejecución
   d. Escritura
10. ¿Qué tipo de permiso se otorga directamente a un archivo o carpeta?
    a. Explícito
    b. Heredado
    c. Efectivo
    d. Compartido
11. Si copia un archivo o carpeta a un nuevo volumen ¿qué permisos tendrá ese archivo o carpeta?
    a. Los mismos permisos que tenía antes
    b. Los mismos permisos que la carpeta de destino

c. Los mismos permisos que la carpeta de origen
d. Ningún permiso en absoluto

12. ¿Cuál de los siguientes utiliza una ACL?
    a. Carpeta NTFS
    b. Usuario de Directorio activo
    c. Clave del registro
    d. Derechos de inicio de sesión
13. ¿Qué tipo de clave tiene una clave para el encriptado y una clave diferente para el desencriptado?
    a. Simétrica
    b. Asimétrica
    c. Función de hash
    d. PKI
14. ¿Qué infraestructura se utiliza para asignar y validar certificados digitales?
    a. Algoritmo asimétrico
    b. Directorio activo
    c. PKI
    d. VPN
15. ¿Qué tecnología se utiliza para encriptar un archivo individual en un volumen NTFS?
    a. BitLocker
    b. BitLocker To Go
    c. PPTP
    d. EFS

Complete los espacios en blanco

Complete los enunciados siguientes escribiendo la palabra correcta o palabras en los espacios en blanco previstos.

1. Una _____ es una contraseña numérica secreta compartida entre un usuario y un sistema que puede utilizarse para autenticar al usuario en el sistema.
2. Una tarjeta de bolsillo con circuitos integrados incrustados que se utiliza para la autenticación se conoce como _____.
3. Un dispositivo que puede darle una segunda contraseña para iniciar sesión en un sistema es _____.
4. El _____ contiene una copia de la base de datos centralizada utilizada en Directorio activo.
5. De forma predeterminada, el reloj de la PC no debe tener más de _____ minutos de error o podría tener problemas con la autenticación con Kerberos.
6. Un_____ define el tipo de acceso sobre un objeto o las propiedades de un objeto, como una impresora o un archivo NTFS.
7. Los permisos _____ fluyen de un objeto primario a un objeto secundario.
8. Cuando no se puede acceder a una carpeta porque alguien quita los permisos para que nadie puede acceder, se debe tomar _____ de la carpeta.

9. La base de datos centralizada que contiene la mayor parte de la configuración de Windows se conoce como la _____.

10. Para realizar el seguimiento de las actividades de un usuario en Windows, se debe habilitar _____.

» Evaluación de Competencias

Escenario 2-1: Comprensión de las desventajas de la biometría

Usted es el administrador de IT para la Contoso Corporation. El CIO quiere investigar el posible uso de la biometría por motivos de seguridad. El CIO comprende qué es la biometría y cómo se puede utilizar esta tecnología, pero él no entiende las potenciales desventajas del uso de la biometría. ¿Qué le debe decir?

Escenario 2-2: Limitación de la auditoría

Usted es el administrador de IT para la Contoso Corporation. El CIO debe saber cuando un usuario accede a una determinada carpeta. Sin embargo, esta información no está disponible porque no se habilitó la auditoría. Para asegurarse de que esto no suceda otra vez en el futuro, el CIO le pide habilitar la auditoría para todo. ¿Cómo debe responder?

» Evaluación de Habilidades

Escenario 2-3: sobre los permisos NTFS

Inicie sesión como administrador en una PC que ejecuta Windows 7 o Windows Server 2008. Cree un grupo denominado Administradores en la PC. Ahora, cree una cuenta de usuario llamada JSmith y asígnela al grupo de Administradores. A continuación, cree otra cuenta de usuario llamada JHamid. Cree una carpeta llamada SharedTest y cree un archivo de texto llamado test.txt en la carpeta SharedTest. Comparta la carpeta. Asigne Permitir Control Total para todo el mundo. Asigne Lectura y Ejecutar para el grupo de Administradores. Inicie sesión como JHamid y trate de acceder a la carpeta \\localhost\SharedTest. A continuación, inicie sesión como JSmith y trate de acceder a la carpeta \\localhost\SharedTest.

Escenario 2-4: sobre EFS

Agregue JHamid al grupo de gestores que se estableció en el ejercicio anterior. Ahora, inicie sesión como JSmith y encripte el archivo test.txt con EFS. Por último, inicie sesión como JHamid y trate de obtener acceso al archivo test.txt.

→ Planificación y mantenimiento de la seguridad

Al considerar la seguridad, es necesario observar todo el cuadro. La seguridad debe planificarse desde el principio. Por lo tanto, es necesario definir cuáles son los objetivos de seguridad, qué impacto tienen sobre el acceso actual y las aplicaciones de red y cómo las medidas de seguridad afectarán a los usuarios. A continuación, después de que dichas medidas se han aplicado, se deben mantener por constante monitoreo de la seguridad del sistema, realizando cambios según sea necesario, aplicando parches de seguridad y revisando constantemente los registros.

Lección 3

Directivas de Seguridad

Matriz para la Lección sobre Capacidad

Capacidad Tecnológica	Dominio del Objetivo	Número de Dominio del Objetivo
Uso de las Directivas de Contraseñas para Mejorar la Seguridad	Comprender las directivas de contraseñas.	2.3

Términos Clave

- Bloqueo de cuenta
- Contraseña crackeada
- Ataque mediante un diccionario
- GPO (Objeto de Directiva de Grupo)
- Capturador de teclado (keylogger)
- Contraseña
- Sniffers (husmeador)
- Contraseña fuerte

Uno de los fundamentos de la seguridad de la información es la protección de redes, sistemas y, ante todo, datos. De hecho, la necesidad de proteger datos es básica para todas las directivas, procedimientos y procesos de seguridad de la información.

La mayoría de la protección de datos de la actualidad se basa en la contraseña. Piense en su vida cotidiana. Utiliza contraseñas para asegurar su correo de voz, su acceso al cajero automático, su cuenta de correo electrónico, su cuenta de Facebook y un servidor de otras cosas. Con el fin de salvaguardar la seguridad de estas cuentas, necesita seleccionar contraseñas fuertes. En esta lección, discutimos lo que implica crear una contraseña fuerte, así como la manera en que puede configurarlas para asegurarse de que permanezcan seguras.

▪ Directivas sobre Contraseñas para Mejorar la Seguridad

↓ EN RESUMEN

Existen diversas configuraciones que puede utilizar en su sistema para asegurarse de que sus usuarios estén obligados a establecer y conservar contraseñas fuertes. Aunque resulte difícil de creer, cuando se les brinda libertad con respecto a sus equipos, muchos usuarios continuarán seleccionando contraseñas débiles al asegurar sus cuentas. Sin embargo, con capacitación a los usuarios y controles del sistema, puede reducir el riesgo de contraseñas débiles que pongan en riesgo sus datos y aplicaciones.

☑ Listo para la Certificación

¿Cómo impone contraseñas más fuertes para su empresa?
—2.3

Un componente básico de su programa de seguridad de información es garantizar que todos los empleados seleccionen y utilicen ***contraseñas fuertes***. La fortaleza de una contraseña se puede determinar observando la longitud, complejidad y aleatoriedad de la misma.

Microsoft brinda algunos controles que se pueden utilizar para asegurar la conservación de la seguridad de las contraseñas, los cuales incluyen controles relacionados con lo siguiente:

- La complejidad de la contraseña
- El bloqueo de cuentas
- La longitud de la contraseña
- El historial de la contraseña
- El periodo comprendido entre cambios de la contraseña
- La exigencia en el uso de las directivas del grupo
- Los métodos de ataque comunes

▶ El nivel de Complejidad de una Contraseña para hacerla más fuerte

La complejidad de la contraseña involucra los caracteres utilizados para crearla. Una contraseña compleja utiliza caracteres de por lo menos tres de las siguientes categorías:

- Caracteres del idioma inglés en mayúscula (“A” a “Z”)
- Caracteres del idioma inglés en minúscula (“a” a “z”)
- Caracteres numéricos (“0” a “9”)
- Caracteres especiales (no alfanuméricos) (!, @, #, $, %, ^, &, etc.)

Cuando se activa, la configuración de complejidad de contraseñas de Microsoft solicita caracteres de tres de estas categorías de manera predeterminada en los controladores de dominio, y el dominio se puede configurar para exigir esta configuración para todas las contraseñas.

Esta configuración puede activarse o desactivarse. No hay configuraciones adicionales disponibles.

Obviamente, aún cuando haga cumplir los criterios de complejidad de la contraseña, no existe garantía de que los usuarios no continuarán utilizando contraseñas que se puedan adivinar con facilidad. Por ejemplo, la contraseña “Verano2010” cumple con los lineamientos de complejidad vigentes requeridos por la configuración de complejidad de contraseñas de Windows; sin embargo, también es una contraseña muy mala porque se puede adivinar fácilmente.

Algunas elecciones de contraseña que deben evitarse incluyen palabras que se pueden encontrar en un diccionario, derivados de nombres de usuarios y secuencias de caracteres comunes, tales como "123456" o "QWERTY." Asimismo, se deben evitar los detalles personales tales como el nombre del cónyuge, el número de placa del automóvil, el número de Seguridad Social o la fecha de nacimiento. Finalmente, debe evitar palabras basadas en nombres propios, ubicaciones geográficas, acrónimos comunes y términos coloquiales.

Algunos métodos recomendados para seleccionar contraseñas fuertes incluyen los siguientes:

- **Cambie los caracteres en una palabra cierto número de letras hacia arriba o hacia abajo en el alfabeto**: Por ejemplo, una traducción mediante un cambio de tres letras de "AArdvark!!" generaría la contraseña "44DDvhzdvo!!"
- **Cree acrónimos a partir de palabras de una canción, poema u otra secuencia familiar de palabras**: Por ejemplo, la frase "¿No preguntes qué puedes hacer por tu país?" podría general la contraseña "Npqphptp?" Agregue "$$" al inicio y obtendrá la contraseña fuerte $$Npqphptp?
- **Combine diversos datos personales, como fechas de nacimiento y colores y comidas favoritos, etc. con caracteres especiales**: Este método generaría contraseñas como "##4Mar!ll0419" o "$^327p!zZ@."

Bloqueo de Cuenta para evitar el Hacking

El Bloqueo de cuenta se refiere al número de intentos de ingreso incorrectos permitidos antes de que el sistema bloquee una cuenta. Cada intento de ingreso equívoco es contabilizado por el contador de ingresos incorrectos y cuando este supera el número de bloqueo de cuenta, no se permiten más intentos. Esta configuración es crítica debido a que uno de los ataques más comunes a las contraseñas (que se discuten más adelante en esta lección) involucra intentar repetidamente el ingreso con contraseñas adivinadas.

Microsoft proporciona tres configuraciones independientes con respecto al bloqueo de cuenta:

- **Duración del bloqueo de cuenta**: esta configuración determina el periodo durante el cual el bloqueo estará vigente antes de que pueda realizarse otro intento de ingreso. Se puede establecer que el periodo sea de 0 a 99,999 minutos. Si se establece un valor de 0, será necesario que un administrador desbloquee la cuenta de manera manual. No tendrá lugar ningún desbloqueo automático.
- **Límite de bloqueo de cuenta**: Esta configuración determina el número de ingresos incorrectos permitidos antes de que se detone el bloqueo de cuenta. Se puede establecer de 0 (sin bloqueo de cuentas) a 999 intentos antes del bloqueo.
- **Restaurar el contador de bloqueo de cuenta posteriormente**: Esta configuración determina el periodo en minutos que debe transcurrir antes de que el contador de bloqueo de cuenta se restaure a 0 intentos de ingreso incorrectos. Si se establece un límite de bloqueo de cuenta, el límite de restauración de bloqueo de cuenta debe ser menor o igual que la duración del bloqueo de cuenta.

Generalmente las configuraciones de bloqueo de cuenta varían entre tres y diez intentos, con una duración del bloqueo de cuenta y una restauración del contador del bloqueo de cuenta de entre 30 y 60 minutos. Aunque algunos usuarios se quejan de que no tienen suficientes intentos de ingreso, esta es una configuración crítica a establecer con el fin de garantizar que su ambiente permanezca seguro.

Longitud de Contraseña

La longitud de una contraseña es un componente clave de su fortaleza y corresponde al número de caracteres utilizados en la misma. Una contraseña con dos caracteres se considera altamente insegura debido a que existe un conjunto muy limitado de contraseñas únicas que se pueden formar utilizando dos caracteres. Por lo tanto, se considera que una contraseña de dos caracteres es fácil de adivinar.

La contraseña de 14 caracteres se encuentra en el polo opuesto. Aunque es extremadamente segura en comparación con una contraseña de dos caracteres, es difícil que los usuarios la recuerden. Cuando las contraseñas se vuelvan tan largas, a menudo los usuarios comienzan a tomar pedazos de papel y escribir sus contraseñas, lo cual ayuda a la pérdida de los beneficios de seguridad que habría obtenido al exigir una contraseña de 14 caracteres en primer lugar.

Tal y como lo ilustran estos casos, el truco para establecer una longitud mínima de contraseña es equilibrar la utilidad con la seguridad. Microsoft le permite establecer una longitud mínima de contraseña de entre 1 y 14 caracteres (una configuración de 0 significa que no se requiere contraseña alguna, lo cual nunca es adecuado en un ambiente de producción). La longitud mínima de contraseña generalmente aceptada es de ocho caracteres.

Historial de Contraseñas para Mantener la Seguridad

El historial de contraseñas es la configuración de seguridad que determina el número de contraseñas únicas que deben utilizarse antes de que alguna ya utilizada anteriormente se pueda reutilizar. Esta configuración evita que los usuarios reciclen las mismas contraseñas en un sistema. Mientras mayor sea el periodo durante el cual se utilice, mayores serán las posibilidades de que se vea comprometida.

Microsoft le permite establecer el valor del historial de contraseñas entre 0 y 24. Diez es una configuración bastante común en ambientes estándar, aunque la configuración predeterminada de Windows Server 2008 es 24 en controladores de dominio.

Tiempo entre Cambios de Contraseñas

★ Tome Nota

Las contraseñas siempre deben expirar, salvo en circunstancias realmente extraordinarias, tales como cuentas de servicios para ejecutar aplicaciones. Aunque esto puede agregar una carga administrativa adicional a algunos procesos, las contraseñas que no vencen pueden ser un serio problema de seguridad en prácticamente todos los ambientes

La última configuración de contraseña con la que debe estar familiarizado es el tiempo entre cambios de contraseña. Esta configuración consta en realidad de dos variantes:

- **Antigüedad Mínima de la Contraseña**: La configuración de antigüedad mínima de la contraseña controla cuántos días deben esperar los usuarios antes de que puedan restaurar su contraseña. Esta configuración puede ser un valor de entre 1 y 998 días. Si se establece en 0, las contraseñas se pueden cambiar inmediatamente. Aunque parece una configuración bastante inocente, un valor muy bajo puede permitir a los usuarios vencer sus configuraciones del historial de contraseñas. Por ejemplo, si establece este valor en 0 y su historial de contraseñas se establece en 10, lo único que los usuarios tienen que hacer es restablecer sus contraseñas 10 veces seguidas y posteriormente volver a su contraseña original. Esta configuración debe establecerse a un valor menor que la antigüedad máxima de la contraseña, salvo que esta se establece en 0, lo que significa que las contraseñas nunca expiran. Diez días o más es generalmente una buena configuración, aunque puede variar ampliamente dependiendo de las preferencias del administrador.
- **Antigüedad Máxima de la Contraseña**: La configuración de antigüedad máxima de la contraseña controla el periodo máximo que puede transcurrir antes de que deba restablecer su contraseña. Esta configuración puede variar entre 1 y 999 días

o se puede establecer en 0 si no desea que sus contraseñas expiren nunca. Una regla general para esta configuración es 90 días para cuentas de usuarios; aunque para cuentas administrativas generalmente es una buena idea restablecer contraseñas de manera más frecuente. En áreas de alta seguridad, se acostumbra una configuración de 30 días.

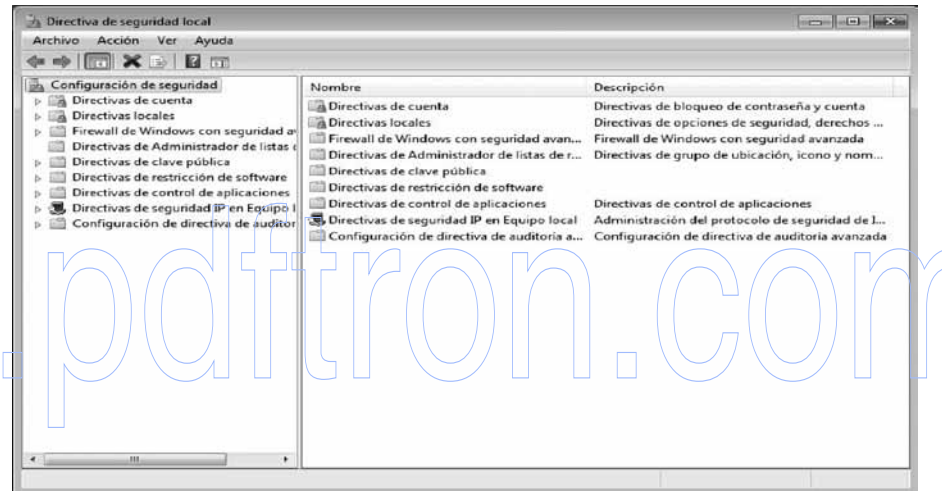
Hemos explicado las distintas configuraciones que puede utilizar para garantizar la mejor seguridad de contraseñas para su ambiente. A continuación, mostraremos cómo revisar estas configuraciones en una estación de trabajo con Windows 7.

→ Configuraciones de Contraseñas en una Estación de Trabajo con Windows 7

PREPÁRESE. Antes de comenzar con estos pasos, asegúrese de ejecutar el complemento insertable **Directiva de Seguridad Local** del menú de **Herramientas Administrativas** (consulte Figura 3-1).

Figura 3-1

Ventana de Directiva de Seguridad Local



1. En el complemento insertable (snap-in) **Directiva de Seguridad Local**, haga clic en **Directivas de Cuenta**.
2. Seleccione **Directiva de Contraseña**. Debe ver las configuraciones de contraseñas que hemos explicado en la ventana derecha. Consulte la Figura 3-2.

Figura 3-2

Configuraciones de seguridad de la Directiva de Contraseñas

3. Haga clic en cada una de las configuraciones de contraseña (consulte las Figuras 3-3, 3-4, 3-5, 3-6 y 3-7 para las distintas configuraciones).

Figura 3-3

Exigir historial de contraseñas

Figura 3-4

Antigüedad máxima de la contraseña

Figura 3-5

Antigüedad mínima de la contraseña

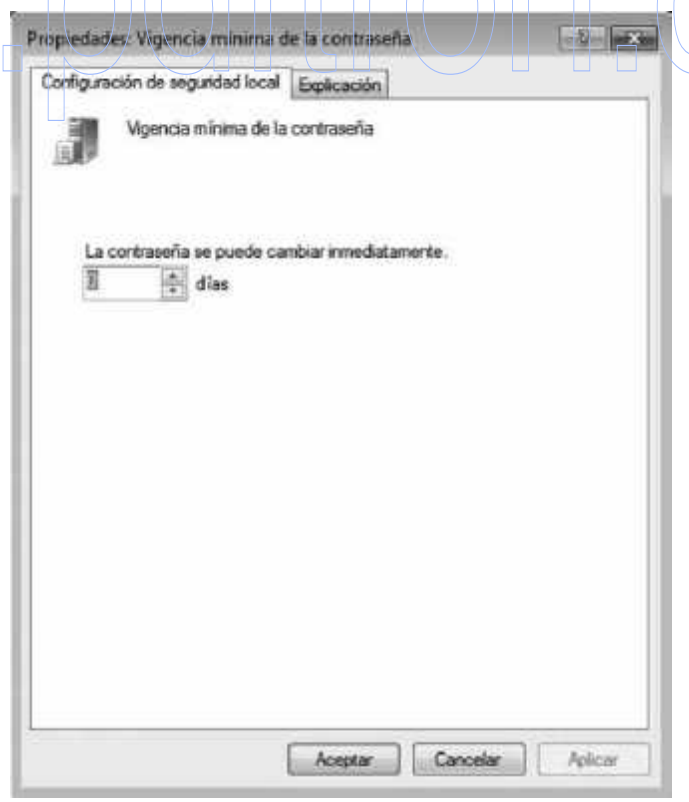


Figura 3-6

Longitud mínima de la contraseña

Figura 3-7

Aplicación de la complejidad de la contraseña

4. Haga clic en **Directiva de Bloqueo de Cuenta**. Verá las configuraciones de bloqueo de cuenta que hemos mencionado en la ventana derecha. Consulte la Figura 3-8.

Figura 3-8

Configuración de la Directiva de Bloqueo de Cuenta

5. Haga clic en cada una de las configuraciones de bloqueo de cuenta mencionadas anteriormente (Consulte las Figuras 3-9, 3-10 y 3-11 para las distintas configuraciones).

Figura 3-9

Umbral de bloqueo de cuenta

Figura 3-10

Duración del bloqueo de cuenta

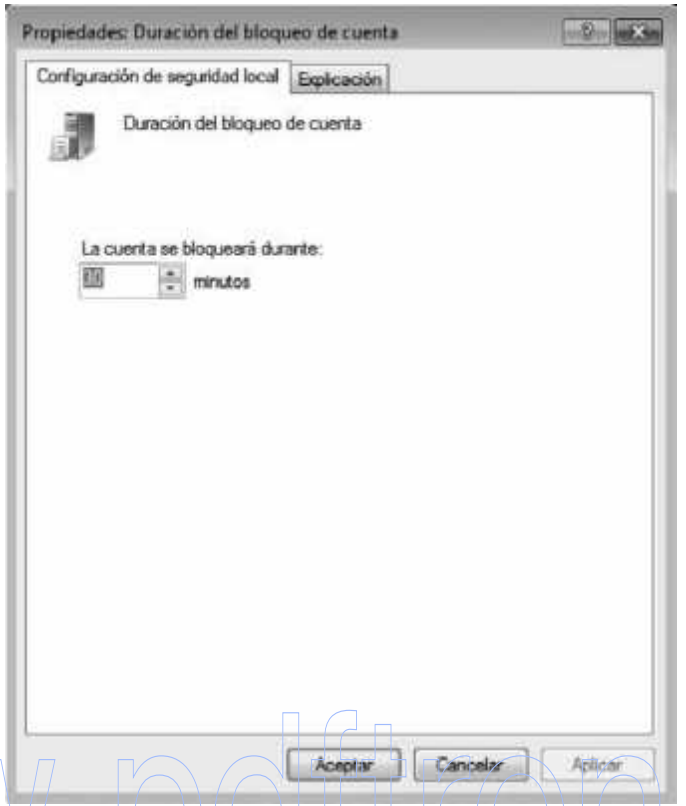
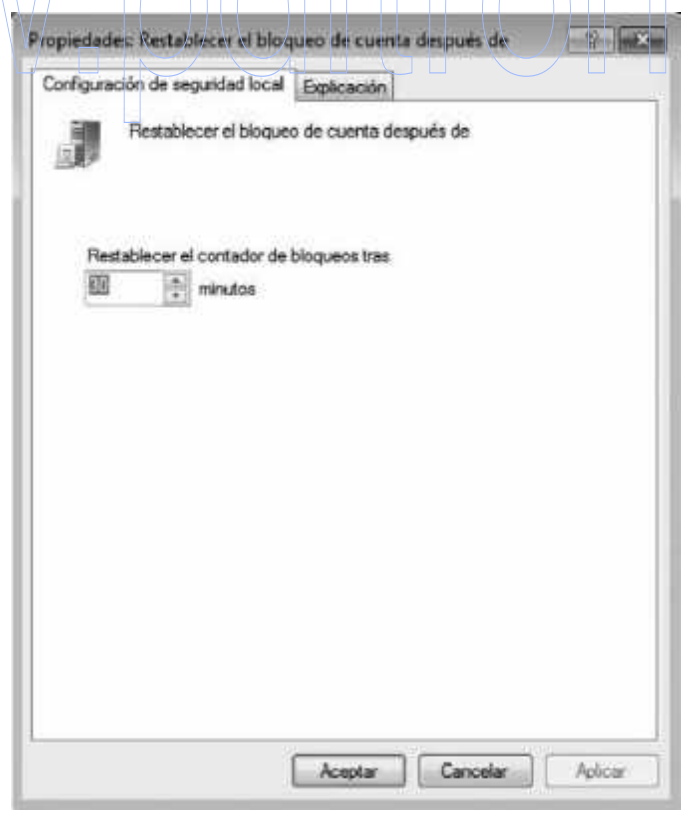


Figura 3-11

Restablecer del temporizador del bloqueo de cuenta



✶ Tome Nota

Las configuraciones de contraseña para un dominio en Windows 2008 son distintas de aquéllas establecidas para un host o cliente individual. En este ejemplo, estamos revisando las configuraciones de contraseña actuales. Revisaremos cómo modificar estas configuraciones utilizando un Objeto de Directiva de Grupo (Group Policy Object, "GPO") en la siguiente Sección

Una vez que hemos revisado el establecimiento de directivas de contraseña en un cliente local, revisemos cómo se pueden utilizar las Directivas de Grupo para establecer estas propiedades para los miembros de un dominio.

▶ *Directivas de Grupo sobre Contraseñas para Mantener la Seguridad*

Antes de estudiar el uso de las Directivas de Grupo para hacer valer las configuraciones de contraseñas, debemos describir exactamente qué es una Directiva de Grupo (también denominada Objeto de Directiva de Grupo).

Un Objeto de Directiva de Grupo (GPO) es un conjunto de reglas que permiten a un administrador un control granular sobre la configuración de objetos en Directorio activo (DA), incluyendo cuentas de usuarios, sistemas operativos, aplicaciones y otros objetos. Los GPO se utilizan para la administración y configuración centralizadas del ambiente del DA.

Ahora que tenemos una mejor idea de lo que es un GPO, analicemos cómo puede utilizar uno para hacer valer los controles de contraseñas en el Directorio activo.

Tome Nota

Windows Server 2008 cambia de manera fundamental el mecanismo para establecer atributos de contraseñas en Directorio activo. Estudiaremos tanto el legado del modelo GPO para aplicar controles de contraseñas como un ejemplo de alto nivel sobre cómo realizar una función similar en un Directorio activo de Windows Server 2008.

→ Directiva de Grupo para Aplicar Controles de Contraseñas sobre Sistemas de Dominio

PREPÁRESE. Antes de comenzar estos pasos, asegúrese de ejecutar el complemento insertable **Usuarios y Computadoras del Active Directory** del menú **Herramientas Administrativas**.

★ Tome Nota

Cuando trabaja con GPO, puede descubrir que sus cambios provocan consecuencias inesperadas. Si un nuevo GPO provoca problemas, desactívelo hasta que tenga una mejor idea de lo que está ocasionando el conflicto

1. Haga clic con el botón derecho en el contenedor raíz (root container) para el dominio y seleccione **Propiedades**.
2. En el cuadro de diálogo de **Propiedades** para el dominio, haga clic en la pestaña **Directiva de Grupo**.
3. Seleccione **Nuevo** para crear un GPO nuevo en el contenedor raíz. Escriba **"Directiva de Contraseñas "** como el nombre de la nueva directiva y haga clic en **Cerrar**.
4. Haga clic con el botón derecho en el contenedor raíz para el dominio y posteriormente seleccione **Propiedades**.
5. En el cuadro de diálogo de **Propiedades**, haga clic en la pestaña **Directiva de Grupo** y posteriormente seleccione su GPO recién creado (denominado Directiva de Contraseñas).
6. Haga clic en **Arriba** para mover su nuevo GPO a la parte superior de la lista.
7. Haga clic en **Editar** para abrir el Editor del **Objeto de Directiva de Grupo** para el GPO que acaba de crear.
8. En la **Configuración de la Computadora**, navegue a la carpeta **Configuración de Windows\Configuración de Seguridad\Directivas de Cuentas\Directivas de Contraseñas**.

9. Desde aquí, puede establecer las directivas como lo hicimos en el ejercicio anterior. Abra cada directiva a su vez, modifique la configuración y haga clic en **Aceptar** para volver al cuadro de diálogo principal.
10. Una vez que haya establecido las configuraciones según lo desee, cierre el **Editor del Objeto de Directiva de Grupo**.
11. Haga clic en **Aceptar** para cerrar el cuadro de diálogo de propiedades del dominio.
12. Salga de **Usuarios y Computadoras de Active Directory**.

Ahora cuenta con un GPO para aplicar las configuraciones de contraseñas. Este proceso funciona muy bien con Windows Server 2003. Sin embargo, con Windows Server 2008 (la versión más reciente del sistema operativo Windows Server), estas directivas requieren un proceso ligeramente diferente.

En particular, Windows Server 2008 le permite almacenar lo que Microsoft denomina directivas de grupo de contraseñas, las cuales le permiten establecer distintas directivas de contraseñas en diferentes contenedores en el Directorio activo. Con el fin de soportar esta nueva funcionalidad, Windows Server 2008 incluye dos nuevas clases de objetos:

- Contenedor de Configuraciones de Contraseñas
- Objeto de Configuraciones de Contraseñas

El Contenedor de Configuraciones de Contraseñas (*Password Settings Container*, "PSC") se crea de manera predeterminada en el contenedor de Sistema en el dominio. Puede verlo utilizando el complemento insertable Usuarios y Computadoras de Active Directory, pero necesitará activar las características avanzadas para acceder al mismo. El PSC almacena los Objetos de Configuraciones de Contraseñas (*Password Settings Objects*, "PSO") para el dominio.

Si no se configuran directivas de contraseñas detalladas, la Directiva de Dominio Predeterminada, también accesible a través del complemento insertable Usuarios y Computadoras de Active Directory, se aplica a todas las cuentas en el dominio.

Analicemos cómo modificar la Directiva de Dominio Predeterminada para lograr una implementación similar al uso del GPO en versiones anteriores del Directorio activo.

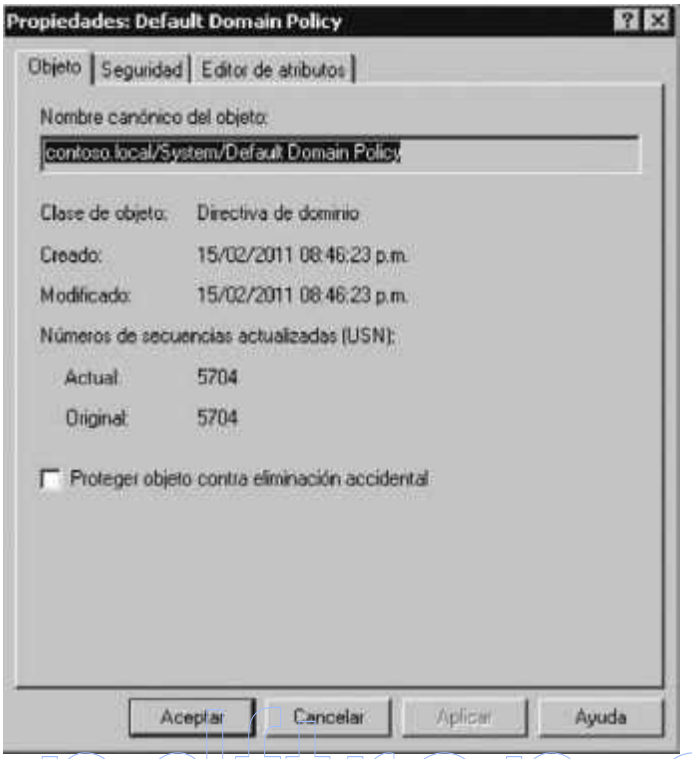
→ Directiva de Dominio Predeterminada (Default Domain Policy) para Aplicar control de Contraseñas en Sistemas de Dominio

PREPÁRESE. Antes de comenzar estos pasos, asegúrese de ejecutar el complemento insertable **Usuarios y Equipos de Active Directory** en las **Características Avanzadas** activado desde el menú de **Herramientas Administrativas**.

1. Despliegue el dominio para mostrar las carpetas predeterminadas.
2. Haga doble clic en **System**. Debe visualizarse la lista de objetos predeterminados en el contenedor del Sistema.
3. Haga clic con el botón derecho en **Default Domain Policy** y seleccione **Propiedades**. Se abrirá el cuadro de diálogo de **Propiedades de Default Domain Policy**. (Consulte la Figura 3-12).

Figura 3-12

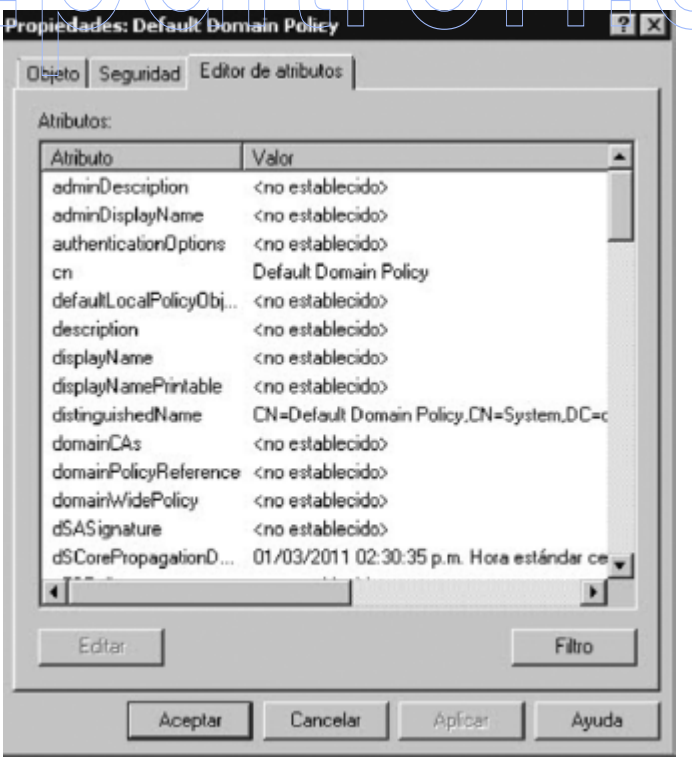
Ficha Objeto del cuadro de diálogo Propiedades: Default Domain Policy



4. Haga clic en la pestaña del **Editor de atributos** y desplácese hacia abajo a **Password Attributes** (Consulte la Figura 3-13).

Figura 3-13

Ficha Editor de atributos del cuadro de diálogo Propiedades: Default Domain Policy



✶ Tome Nota

La nueva funcionalidad de Windows Server 2008 brinda beneficios significativos a administradores experimentados del Directorio activo, pero puede crear una complejidad importante para una persona no familiarizada con DA. Realice los cambios con precaución

5. Haga doble clic en el atributo que desee modificar.
6. Cuando haya completado los cambios deseados, haga clic en **Aceptar** para cerrar el cuadro de diálogo de **Propiedades: Default Domain Policy**.
7. Salga de **Usuarios y Equipos de Active Directory**.

Ahora que conoce algunas maneras de establecer atributos de contraseña para el cliente, tanto en un Directorio activo en Windows Server 2003 como en la versión actual del mismo, es necesario analizar algunos de los métodos de ataque más comunes que podría encontrar en el mundo real.

▶ *Los Métodos de Ataque Comunes*

Desde hace tiempo, las contraseñas se han considerado uno de los eslabones débiles en diversos programas de seguridad. Aunque los *tokens*, tarjetas inteligentes y la información biométrica están ganando impulso en el mundo comercial para asegurar los sistemas y datos clave, una cantidad significativa de datos confidenciales y privados continúan asegurándose mediante contraseñas. Estas se consideran un eslabón débil principalmente por dos motivos:

En primer lugar, algunas personas se basan completamente en los usuarios para la selección de contraseñas, aunque muchos elegirán contraseñas fuertes acorde a sus estándares y aunque podrían contar con algunas herramientas para aplicar atributos de contraseñas (como la complejidad y longitud mínima), seguirá habiendo usuarios que continúen seleccionado contraseñas débiles. Los atacantes lo saben y tratarán de explotar a estas personas.

En segundo lugar, incluso las contraseñas fuertes son vulnerables a ataques a través de una variedad de distintos mecanismos.

Análisis de Ataques mediante un Diccionario y con Fuerza Bruta

Un ***ataque mediante un diccionario*** utiliza un diccionario que contiene una lista de contraseñas potenciales que el atacante prueba en conjunción con un nombre de usuario en un intento por adivinar la contraseña correspondiente. Esto se conoce como un ataque mediante un diccionario debido a que las versiones más antiguas de este realmente utilizaban listas de palabras tomadas de un diccionario como base de su intento de ingreso. Actualmente, existen diccionarios personalizados con contraseñas probables disponibles para descarga a través de Internet, junto con aplicaciones que pueden utilizar estas posibles contraseñas contra sus sistemas.

Otro tipo más agresivo de ataque (denominado un ataque con fuerza bruta) no se basa en una lista de contraseñas, sino que prueba todas las combinaciones posibles de tipos de caracteres permitidos. Aunque históricamente este tipo de ataque se consideraba no efectivo, las mejoras en el desempeño del procesador y la red lo han hecho más útil, aunque no tan efectivo como un ataque mediante un diccionario.

Estos tipos de ataques tienden a tener mayor éxito cuando la longitud de la contraseña es de siete caracteres o menos. Cada carácter adicional agrega un número importante de contraseñas posibles. Estos ataques a menudo tienen éxito debido a que los usuarios a veces

utilizan palabras comunes con la primera letra en mayúscula y posteriormente agregan un número para cumplir con los lineamientos de complejidad. Estas son las contraseñas más fáciles de recordar para los usuarios, pero también son las más fáciles de comprometer para un atacante.

La configuración de Bloqueo de Cuenta analizada anteriormente en la lección es una defensa de suma importancia contra este tipo de ataque debido a que un Bloqueo de Cuenta disminuirá o incluso detendrá un ataque con fuerza bruta en ejecución después de que se alcance el número de intentos de ingreso incorrectos.

Ataques Físicos

Siempre que un atacante tenga acceso físico a su equipo de cómputo, éste se encuentra en riesgo. Los ataques físicos a su computadora pueden superar completamente casi todos mecanismos de seguridad, por ejemplo mediante la captura de contraseñas y otros datos críticos directamente del teclado cuando se utiliza un software o hardware ***capturador de teclado (keylogger).*** De hecho, si su clave de encriptado pasa a través de un keylogger, puede descubrir que incluso sus datos encriptados se encuentran en riesgo.

Referencia Cruzada

La lección 1 contiene más detalles sobre el keylogging.

Algunos otros ataques físicos pueden incluir el uso de una cámara oculta para grabar lo que escribe en el teclado o incluso la remoción o duplicación (o robo directo) de su disco duro. Aunque no se trata específicamente de un ataque contra una contraseña, si los atacantes remueven su disco duro, con frecuencia pueden evadir los controles de contraseñas mediante el montaje de la unidad de manera remota y accediendo a sus datos directamente de la unidad, sin que intervenga el sistema operativo.

Contraseñas Divulgadas sin Autorización y Compartidas

Otro desafío que encontrará al participar con usuarios en un ambiente de oficina es el hecho de que una contraseña sea compartida o divulgada sin autorización. Los usuarios tienden a confiar en sus compañeros de trabajo; después de todo, todos trabajan para la misma empresa y, en muchos casos, tienen acceso a información similar de la empresa. Como resultado de lo anterior, los usuarios pueden ser convencidos fácilmente de que compartan sus contraseñas con compañeros de trabajo que creen que "necesitan" esta información. Esta práctica es especialmente problemática en ambientes con alta rotación de personal debido a que no existe manera de saber quién de entre el último grupo de empleados despedidos todavía cuenta con el nombre de usuario y contraseña de un amigo y en consecuencia cuenta con acceso continuo a la red.

Aún cuando los usuarios no proporcionen su contraseña a otro empleado de manera intencional, el ambiente laboral casual con frecuencia provoca que los empleados observen a sus compañeros de trabajo al escribir sus nombres de usuario y contraseñas.

Finalmente, los cónyuges, hijos y otros parientes pueden llegar a tener acceso a su ambiente de cómputo debido a su estrecha relación con sus empleados.

La conciencia por parte de los empleados es la mejor manera de combatir este tipo de ataque. Proporcionar a los empleados un mayor entendimiento de los riesgos e impacto de este tipo de comportamientos puede ser de gran utilidad para la conservación de las contraseñas bajo el control exclusivo de usuarios autorizados. Además, las configuraciones de antigüedad mínima y máxima de la contraseña, además de la configuración del historial de la contraseña, pueden ayudar a mitigar este riesgo. En este caso, aún cuando alguien obtenga una contraseña que no debería tener, cuando se alcanza el límite de antigüedad máximo se deberán restaurar todas, incluidas las compartidas.

Contraseñas Crackeadas

Una ***contraseña crackeada*** se basa con frecuencia en más que un simple ataque a la contraseña. En un ataque de crackeo, el atacante obtiene acceso a un archivo encriptado de contraseñas de una estación de trabajo o servidor. Una vez que ha logrado ingresar, el atacante comienza a ejecutar herramientas de crackeo de contraseñas contra el archivo con el fin de violar tantas como sea posible y utilizarlas a su favor para comprometer aún más la red y sistemas de la empresa.

Las contraseñas almacenadas en un estado encriptado son más difíciles de violar que las almacenadas en un texto claro o en un estado *hashed*. Sin embargo, con el poder actual de las computadoras, incluso los almacenamientos de contraseñas encriptados se ven amenazados por ataques de crackeo.

Si en algún momento se da cuenta de que su contraseña se ha visto comprometida, necesita que todos los empleados con una cuenta en el mismo sistema cambien sus contraseñas de manera inmediata.

También puede utilizar las mismas herramientas que los atacantes potenciales para auditar la seguridad de sus almacenamientos de contraseñas. Tratar de crackear su propio archivo de contraseñas es una práctica bastante común, dado que no sólo le permite someter a prueba la seguridad de su almacenamiento sino que también, si cualquiera de estas se ve comprometida o si es débil, le brinda la posibilidad de hacer que los usuarios las cambien por unas más seguras.

Examen de Sniffers de Red e Inalámbricos

Si un atacante logra acceder a su red interna, a su red inalámbrica o incluso a un punto de acceso de Internet utilizado por sus empleados, tiene la capacidad de utilizar una herramienta especializada denominada *sniffer* para tratar de interceptar contraseñas no cifradas. Aunque las aplicaciones han mejorado en los años recientes, continúa habiendo varias de ellas que transmiten información importante (como contraseñas) a través de redes en texto claro, lo cual significa que esta información puede ser leída por cualquier persona con la capacidad de ver datos conforme atraviesen la red.

Los ***Sniffers*** son aplicaciones de software (y en algunos casos de hardware) especialmente diseñadas que capturan paquetes de red conforme atraviesan una red, mostrándolos al atacante. Los *sniffers* son formas válidas de equipo de prueba utilizadas para identificar problemas de red y aplicación; sin embargo, los atacantes se han adueñado rápidamente de la tecnología como una manera sencilla de obtener credenciales de ingreso.

Además de los *sniffers* que se utilizan para atacar redes alámbricas, ahora existen *sniffers* que tiene la capacidad de capturar también datos inalámbricos. Cuando se conecta a la red inalámbrica de su negocio, posiblemente mientras se encuentra en la cafetería local o incluso cuando asiste a una reunión en un hotel, se encuentra en riesgo potencial de que sus datos sean literalmente extraídos del aire y puestos a disposición de un atacante. El uso del encriptado sigue siendo el mejor mecanismo para combatir este tipo de ataque.

Otra área de riesgo con los *sniffers* son los teclados inalámbricos. En su núcleo, un teclado inalámbrico es una tecnología emisora que envía las pulsaciones de las teclas del teclado a un receptor conectado a la computadora. Si puede sintonizar un receptor a la misma frecuencia lo suficientemente cerca de la computadora, puede capturar cada golpe del teclado ingresado en el teclado inalámbrico sin necesidad de instalar un *keylogger*. Actualmente, la mayoría de los teclados soportan seguridad adicional (por ejemplo, conexiones cifradas),

pero siguen emitiendo toda la información que el usuario escribe, de modo que en tanto la gente continúe ingresando la mayoría de sus datos a través del teclado seguirá existiendo una fuente potencial significativa para que los atacantes la exploten. De hecho, muchas empresas permiten que sus empleados utilicen teclados alámbricos a fin de disminuir este riesgo.

Referencia Cruzada

El *sniffing* se analiza a mayor detalle en la Lección 4.

Contraseñas Adivinadas

Aunque ya no es un problema tan frecuente como en años pasados, sigue existiendo la posibilidad de que alguien pueda sentarse frente a su computadora y adivine su contraseña. Como lo hemos visto en numerosas películas, un atacante puede estar familiarizado con la persona cuyo sistema esté tratando de comprometer o podría mirar a su alrededor y ver una postal de un viaje o fotografías de los hijos de un empleado con sus nombres enlistados y discernir la contraseña a partir de estos elementos. Si un usuario no cumple con las normas corporativas que exigen una contraseña fuerte que no se pueda adivinar fácilmente y en vez de ello selecciona una contraseña basada en el nombre o cumpleaños del cónyuge, hijos o mascota, un atacante puede adivinar más fácilmente la contraseña y obtener acceso a los datos del empleado.

Dicho lo anterior, este tipo de ataque casi nunca se observa actualmente. Con la amplia disponibilidad de herramientas de crackeo, el tipo de objetivo individual requerido para adivinar la contraseña de una persona rara vez vale la pena el esfuerzo. Generalmente es mucho más sencillo apalancar un ataque utilizando uno de los demás métodos disponibles actualmente. En general, únicamente los compañeros de trabajo o amigos cercanos intentarán adivinar la contraseña de un empleado.

Resumen de Capacidad

En esta lección, aprendió lo siguiente:

- La fortaleza de una contraseña puede determinarse observando su longitud, complejidad y aleatoriedad.
- Una contraseña compleja utiliza caracteres de por lo menos tres de las siguientes categorías: mayúscula, minúscula, caracteres numéricos y caracteres especiales (no alfanuméricos).
- Bloqueo de cuenta se refiere al número de intentos de ingreso incorrectos antes de que un sistema bloquee una cuenta.
- La Antigüedad Mínima de la Contraseña controla cuántos días deben esperar los usuarios antes de poder restaurar su contraseña.
- La Antigüedad Máxima de la Contraseña controla el periodo máximo que puede transcurrir antes de que los usuarios estén obligados a restaurar su contraseña.
- Un Objeto de Directiva de Grupo (GPO) es un conjunto de reglas que permiten a un administrador tener un control detallado de la configuración de objetos en el Directorio activo (DA), incluyendo cuentas de usuarios, sistemas operativos, aplicaciones y otros objetos.
- Las contraseñas se han reconocido por largo tiempo como uno de los eslabones más débiles en diversos programas de seguridad.

- Durante un ataque mediante un diccionario, el atacante prueba una amplia lista de contraseñas potenciales en conjunción con un nombre de usuario para tratar de adivinar la contraseña correspondiente.
- Los ataques con fuerza bruta prueban todas las combinaciones posibles de tipos de caracteres permitidos en un intento por determinar la contraseña de un usuario.
- Los ataques físicos a una computadora pueden evadir completamente casi todos los mecanismos de seguridad, por ejemplo mediante la captura de contraseñas y otros datos críticos directamente de un teclado cuando se utiliza un software o hardware *keylogger*.
- En un ataque de crackeo de contraseña, los atacantes obtienen acceso a un archivo encriptado de contraseñas de una estación de trabajo o servidor. Una vez que tienen acceso a este archivo, los atacantes comienzan a ejecutar herramientas de crackeo de contraseñas contra el mismo.
- Si obtiene acceso a su red interna, su red inalámbrica o incluso a un punto de acceso de Internet utilizado por sus empleados, el atacante tiene la capacidad de utilizar una herramienta especializada denominada *sniffer* a fin de interceptar contraseñas no cifradas.
- Aunque ya no es un problema tan frecuente como en años pasados, sigue existiendo la posibilidad de que alguien pueda sentarse frente a su computadora y adivine su contraseña.

» Evaluación de Conocimientos

Opción Múltiple

Encierre en un círculo la letra o letras que correspondan a la mejor respuesta o respuestas.

1. ¿Cuáles de los siguientes no son controles de contraseñas válidos? (Elija todos los aplicables)
   a. Antigüedad Mínima de la Contraseña
   b. Antigüedad Máxima de la Contraseña
   c. Longitud Máxima de la Contraseña
   d. Límite de Bloqueo de Cuenta
   e. Historial de Contraseñas
2. ¿Cuál(es) de las siguientes sería una contraseña aceptable en un sistema Windows 7 Professional con Complejidad de la Contraseña activada y una Longitud Mínima de la Contraseña establecida en ocho? (Elija todas las opciones correctas)
   a. Verano2010
   b. $$Thx17
   c. ^^RGood4U
   d. Contraseña
   e. St@rTr3k
3. ¿Cuál es la configuración máxima para la Antigüedad Mínima de la Contraseña?
   a. 14
   b. 999
   c. 998
   d. 256

4. Está configurando su primera estación de trabajo segura con Windows 7 Professional y está estableciendo el historial de contraseña. ¿Cuáles son las configuraciones mínima y máxima que puede utilizar? (Elija la mejor respuesta)

   a. 0, 14
   b. 1, 14
   c. 0, 24
   d. 1, 24
   e. 0, 998

5. ¿Cuáles de los siguientes son tipos comunes de ataques a contraseñas? (Elija Dos respuestas)

   a. Crackeo
   b. *Man in the middle*
   c. *Smurf*
   d. *Spoofing*

6. Una forma de ataque con fuerza bruta contra contraseñas utiliza una amplia lista de contraseñas predefinidas. ¿Cómo se denomina esta forma de ataque con fuerza bruta? (Elija la mejor respuesta)

   a. Ataque mediante la Biblia
   b. Ataque de crackeo
   c. Ataque mediante adivinanzas
   d. Ataque mediante un diccionario

7. En su calidad de Director de Seguridad de una pequeña empresa de procesamiento de registros médicos, sospecha que un competidor atacará su red muy pronto. Al haber trabajado en el negocio por un tiempo, está bastante seguro de que el competidor intentará de ejecutar un ataque mediante diccionario contra uno de sus servidores de aplicaciones de Windows. Desea asegurarse de que su competidor no logre tener acceso al servidor utilizando este método de ataque. ¿Qué configuración debe ajustar con el fin de garantizar que este ataque tenga una oportunidad limitada de éxito? (Elija la mejor respuesta)

   a. Longitud Mínima de la Contraseña
   b. Límite de Bloqueo de Cuenta
   c. Historial de Contraseñas
   d. Antigüedad **Máx**ima de la Contraseña

8. Es el responsable del departamento de seguridad corporativa y el equipo de Microsoft la ha solicitado asistencia en el establecimiento de los controles de contraseñas en su nuevo servidor independiente (*stand-alone*). ¿Qué Herramienta Administrativa debe utilizar para establecer estas configuraciones?

   a. Usuarios y Equipos de Active Directory
   b. Administración del Equipo de Cómputo
   c. Servicio de Seguridad
   d. Directiva de Seguridad Local

9. ¿Cuáles son las dos nuevas características introducidas en Windows Server que permiten el uso de directivas de seguridad detalladas? (Elija todas las aplicables)

   a. Objeto de Directiva Global
   b. Contenedor de Configuraciones de Contraseña

c. Objeto de Configuraciones de Contraseña
d. Directiva de Contraseña

10. ¿Por qué utilizaría una Antigüedad Mínima de Contraseña?
    a. Para garantizar que nadie adivine una contraseña
    b. Para evitar que alguien intente una y otra vez adivinar una contraseña
    c. Para asegurarse de que un usuario no restaure una contraseña varias veces hasta que pueda reutilizar su contraseña original
    d. Para restaurar automáticamente una contraseña

Complete las oraciones

1. Un conjunto de reglas que permite a un administrador tener un control detallado de la configuración de objetos en Directorio activo (DA), incluyendo cuentas de usuario, sistemas operativos, aplicaciones y otros objetos de DA se denomina _____.
2. El número de intentos de ingreso incorrectos permitidos antes de que un sistema bloquee una cuenta se denomina _____.
3. La configuración que determina el número de contraseñas únicas que deben utilizarse antes de que una contraseña se pueda re-utilizar es _____.
4. El tipo de ataque que utiliza una amplia lista de contraseñas potenciales se denomina _____.
5. Cuando utiliza software especial para leer datos conforme se emiten en una red, está _____ la red.
6. El (la) _____ necesita ser menor o igual que la Duración del Bloqueo de Cuenta.
7. La configuración más alta que puede utilizar la Duración del Bloqueo de Cuenta es _____.
8. En un Directorio activo en Windows Server 2008, el (la) _____ se aplica automáticamente en caso de que no haya establecido una directiva de contraseña detallada.
9. Las tres configuraciones para el bloqueo de cuenta son _____, _____ y _____.
10. Una cuenta _____ es un tipo de cuenta que puede configurar de modo que la contraseña no expire.

» Evaluación de Competencia

Caso 3-1: Contraseñas Largas

a. Digamos que tiene un PIN que tiene cuatro dígitos de longitud. Cada dígito puede ser 0, 1, 2, 3, 4, 5, 6, 7, 8 ó 9, dando un total de 10 dígitos posibles. ¿Cuántos PIN distintos son posibles?
b. Digamos que tiene una contraseña de cuatro letras y cada carácter en la contraseña debe ser una letra minúscula (a–z). Existen 26 letras en el alfabeto. ¿Cuántas contraseñas diferentes son posibles?

c. Digamos que tiene una contraseña de seis letras y cada carácter en la contraseña debe ser una letra minúscula (a–z). ¿Cuántas combinaciones diferentes son posibles?

d. Digamos que tiene una contraseña de ocho letras y cada carácter en la contraseña debe ser una letra minúscula (a–z). ¿Cuántas combinaciones diferentes son posibles?

e. Digamos que tiene una contraseña de ocho letras y cada carácter debe ser una letra minúscula (a–z) o una letra mayúscula (A–Z). ¿Cuántas combinaciones diferentes son posibles?

f. Digamos que tiene una contraseña de ocho letras y cada carácter en la contraseña debe ser una letra en minúscula (a–z), una letra en mayúscula (A–Z), un dígito (0–9) o un carácter especial (~`!@#$%^&*()_-+={[}]|\:;"'<,>.? ó /). ¿Cuántas combinaciones diferentes son posibles?

Caso 3-2: Cambio de Contraseñas

Imagine que trabaja para Contoso Corporation. Su Director de Informática le dice que acaba de recibir un mensaje en su computadora indicando que debe cambiar su contraseña. Él desea saber por qué no sólo debe utilizar una contraseña relativamente larga sino también por qué debe cambiarla de manera regular. ¿Qué debe decirle?

» Evaluación de Habilidad

Caso 3-3: Administración de los Usuarios

Ingrese a una computadora que opere con Windows 7 y cree una cuenta para John Adams (JAdams) utilizando el Panel de Control. Agregue a JAdams al grupo del Administrador. Configure la contraseña para esta persona como Contraseña01. Verifique que los grupos de los que sea miembro JAdams utilizando el Control de Administración del Equipo.

Caso 3-4: Configuración de una Directiva de Seguridad Local

En una computadora que opere con Windows 7, abra la Administración de Directivas de Grupo para ingresar a la Directiva Local de Grupo. Consulte la Directiva de Contraseña y la Directiva de Bloqueo de Cuenta.

Listo para el Lugar de Trabajo

→ Directivas de Grupo

Las Directivas de Grupo son parte de las características más poderosas incluidas con Directorio activo. Además de ser utilizadas para configurar las directivas de contraseña y las directivas de bloqueo de cuenta, se pueden utilizar para asignar derechos de usuario que definan lo que una persona puede realizar en un equipo de cómputo. También se pueden utilizar para instalar software, evitar la instalación de software, bloquear una computadora, estandarizar un entorno de trabajo y pre-configurar Windows. Cuando analice con mayor detalle las Directivas de Grupo, verá que existen literalmente miles de configuraciones.

Lección 4

Seguridad en la Red

Lección de la matriz de habilidades

Habilidades tecnológicas	Dominio del objetivo	Número de dominio del objetivo
Utilizar firewalls dedicados para proteger una red	Comprender los cortafuegos dedicados.	3.1
Controlar el acceso con Protección de acceso a redes (NAP)	Comprender la Protección de acceso a redes (NAP).	3.2
Utilizar el aislamiento para proteger la red	Comprender el aislamiento de la red.	3.3
Proteger los datos con la seguridad del protocolo	Comprender la seguridad del protocolo.	3.4
Proteger la red inalámbrica	Comprender la seguridad de la red inalámbrica.	1.4

Términos clave

- Cortafuegos a nivel de aplicación (firewall a nivel de aplicación)
- Cortafuegos a nivel de circuito (firewall a nivel de circuito)
- Zona desmilitarizada (DMZ)
- Extensiones de seguridad de DNS (DNSsec)
- Ataques de envenenamiento de DNS (DNS poisoning)
- Suplantación de DNS (DNS Spoofing)
- Cortafuegos (firewall)
- Honey net
- Honeypot
- Cortafuegos de servidor (firewall de servidor)
- Sistemas de detección de intrusos (IDS)
- Sistemas de prevención de intrusos (IPS)
- MAC Address
- Protección de acceso a redes (NAP)
- Cortafuegos de red (firewall de red)
- Modelo de interconexión de sistemas abiertos (OSI)
- Padded cell (célula de aislamiento)
- Cortafuegos personal (firewall personal)
- Suplantación (Spoofing)
- Stateful Inspection

Tradicionalmente, cuando se construía una infraestructura de seguridad de información, el primer punto de enfoque era la red. Tan pronto como las redes comenzaron a interconectarse, fue obvio que las mismas ofrecían el principal vector de ataque. En otras palabras, era la principal manera de obtener información de una organización desde el exterior.

En ese momento, la filosofía impulsora alrededor de la protección de las redes era reminiscente de los castillos de antaño. De acuerdo con este modo de pensar, la mejor manera de asegurar tu red era construir un muro fuerte, cavar fosos y controlar el acceso al castillo a través de un portón principal. En términos de redes, esto significaba desplegar varias capas de cortafuegos, después controlar quién podría entrar en la red con sus reglas, controles de acceso y zonas desmilitarizadas (DMZs). Esta práctica es conocida como asegurar el perímetro o defensa en profundidad.

Este modelo trabajó bastante bien hasta la siguiente ronda de evolución tecnológica a finales de la década de 1990, cuando se introdujo el concepto de red privada virtual (VPN). Las VPNs permiten a las compañías extender de manera segura su red a través de redes que no son de confianza, como el Internet, pero esto también impactó el perímetro de la red. Después vinieron las tecnologías de red inalámbrica, literalmente movieron el perímetro que requería protección en el aire y ofrecieron retos adicionales al modelo de seguridad en capas.

La buena noticia es que como las tecnologías de redes han evolucionado y el asegurar un perímetro de redes se ha vuelto más desafiante, las tecnologías de seguridad disponibles para dirigir estos retos también han evolucionado. En esta lección, discutiremos dichas soluciones de seguridad y cómo se pueden utilizar para dirigir los desafíos que se encontrarán.

▪ Utilizar Cortafuegos (firewalls) dedicados para proteger una Red

↓ EN RESUMEN

Incluso hoy, los cortafuegos siguen siendo los cimientos de la tecnología de seguridad de redes. Hay muchas opciones, tipos y tecnologías relacionadas con la selección, implementación y mantenimiento de firewalls en la red. También hay muchos controladores para ayudar a determinar la solución adecuada para una organización.

☑ Listo para la Certificación

¿Dónde ubicaría la mayoría de las compañías su firewall dedicado?
—3.1

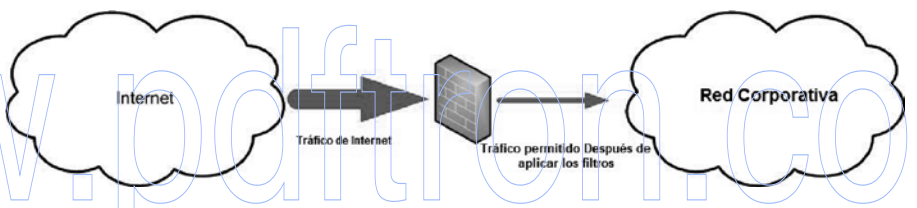
Uno de los primeros aspectos que surge cuando la gente habla de seguridad de información son los cortafuegos. Estos han sido durante mucho tiempo el fundamento de la infraestructura de la seguridad de redes de una organización. Pero, ¿qué es exactamente un cortafuegos?

Un ***cortafuegos o firewall*** es un sistema que está diseñado para proteger una computadora o una red de computadoras de los ataques basados en la red. Un firewall hace esto filtrando los paquetes de datos que atraviesan la red. Un cortafuegos de perímetro típico esta implementado con dos (o más) conexiones de redes (ver Figura 4-1), concretamente:

- Una conexión a la red que se está protegiendo y
- Una conexión a una red externa.

Figura 4-1

Implementación de cortafuegos



Hay diversas variaciones en este modelo, pero a la larga, todos los cortafuegos protegen los servidores en una red de los servidores de otra red.

Se utilizan para dividir y aislar las áreas de red de una organización. Por ejemplo, uno de los usos más comunes de un cortafuegos sería dividir la red de su organización (red interna) de la red externa (Internet). La red interna quizá podría ser referida como limpia, segura y local, mientras que la red externa tal vez podría ser referida como sucia, insegura y remota. Todas se refieren al mismo modelo, pero, ocasionalmente, quizá podría hallar que necesita ayuda para traducir un término particular a una terminología con la que se esté familiarizado.

En las redes de hoy en día, hallará cortafuegos utilizados para varios propósitos más allá de sólo asegurar el perímetro. Por ejemplo, muchas redes de corporativos están divididas en zonas aseguradas por ellos. De este modo, tal vez pueda encontrar que los firewalls de su organización no sólo están asegurando las conexiones de extranet e Internet, sino también creando zonas seguras para sus sistemas financieros, asegurando la investigación y desarrollo de servidores o tal vez incluso la red de producción de las redes de prueba y desarrollo.

Dados los usos ampliamente variables de los cortafuegos en las redes actuales, hay una variedad de diferentes tipos. Pero antes de comenzar a hablar de estos, necesitamos discutir el modelo OSI.

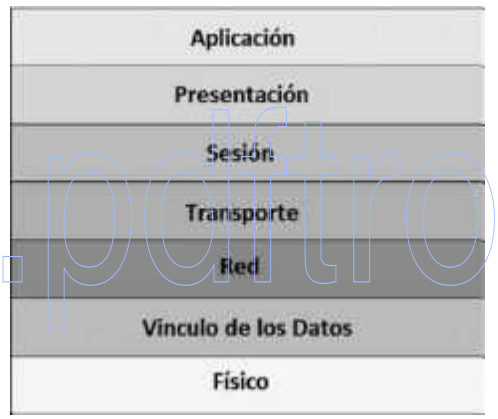
Comprensión del Modelo OSI

Toda discusión respecto a la seguridad de redes requiere una comprensión del modelo de referencia de **interconexión de sistema abierto (OSI)**. El modelo OSI es un modelo conceptual, creado por la Organización Internacional de Estandarización (ISO) en 1978 y revisado en 1984, para describir una arquitectura de red que permita el tránsito de datos entre los sistemas de computadoras. Aunque nunca se utilizó completamente como modelo para un protocolo, no obstante, el modelo OSI es el estándar para discutir cómo trabajan las redes.

Como se muestra en la Figura 4-2, el modelo OSI está integrado de la misma manera como se discute generalmente, de abajo hacia arriba. Las siete capas de este modelo son las siguientes: física, enlace de datos, red, transporte, sesión, presentación y aplicación. Aquí, la capa física se conoce como capa 1, el enlace de datos como la capa 2, etcétera. Esto es importante para recordar, ya que con frecuencia oirá que a los routers (también conocidos como ruteadores o enruteadores) se les dice "dispositivos de capa 3" o tipos específicos de cortafuegos descritos como "dispositivos de capa 7". Esta nomenclatura hace referencia al nivel donde interactúa el dispositivo en el modelo OSI. Por consiguiente, es importante familiarizarse con el concepto de alto nivel del modelo OSI y de lo que sucede en cada capa.

Figura 4-2

Modelo OSI de siete capas



Cada capa del modelo OSI tiene su propia función específica. Las siguientes secciones describen la función de cada capa, comenzando con la capa física y trabajando hacia arriba.

Capa física (capa 1)

★ Tome nota

Los estándares IEEE 802.x definen una variedad de tecnologías de redes. Por ejemplo, 802.1x define un estándar para la seguridad inalámbrica. De manera similar, el estándar IEEE 802.3 define el Ethernet

La capa física del modelo OSI se utiliza para definir las características físicas de la red, incluyendo las siguientes especificaciones:

- **Medio:** Tipos de cables, voltaje, frecuencia de señal, velocidad, ancho de banda, etc.
- **Hardware:** Tipo de conector, tipo de tarjeta de interfaz de red, etc.
- **Topología:** La topología utilizada en la red, como anillo, malla, estrella o bus.

Capa de vínculo de los datos (capa 2)

La capa de enlace de datos conecta la capa de datos con la física, para que puedan transmitirse a través de la red. La capa de enlace de datos maneja la detección de errores, su corrección y la dirección de hardware (es decir, la dirección de la tarjeta de interfaz de la red).

La capa de enlace de datos se divide en dos subcapas:

- **Subcapa de Control de Acceso al Medio (MAC)**: La *MAC address* se define en esta capa. Es la dirección física o la dirección de hardware plasmada en cada tarjeta de interfaz de red-NIC (por ejemplo: 96-4C-E5-48-78-C7). También controla el acceso a los medios de redes subyacentes.
- **Subcapa de control de enlace lógico (LLC)**: La capa LLC es la responsable del los mecanismos de control de flujo y errores de la capa de enlace de datos. La capa LLC esta especifica en el estándar IEEE 802.2.

Capa de red (capa 3)

La capa de red es la principal responsable del enrutamiento. Esta capa define los mecanismos que permiten que los datos pasen de una red a otra. Para aclarar, esta capa no especifica cómo se pasan los datos; sino, define los mecanismos que permiten este tránsito. El cómo se pasan los datos se define mediante los protocolos de enrutamiento (de los cuales se hablará con más detalle posteriormente en la lección). Como resultado, un router se conoce típicamente como un dispositivo de capa 3.

Tome nota

Es importante recordar que además del enrutamiento (permitiendo al tráfico seleccionar el mejor camino), la capa de red del modelo OSI especifica otra función crítica: direccionar. En el caso de TCP/IP, ésta es la capa donde se especifican las direcciones IP. Aunque la capa de enlace de datos utiliza direcciones MAC hard-code para comunicar en la capa física, los protocolos de red utilizan direcciones configuradas por software y enrutan protocolos para comunicarse a través de la red

Capa de transporte (capa 4)

La capa de transporte hace exactamente lo que su nombre implica: proporciona los mecanismos para llevar datos a través de una red. Esta capa utiliza tres mecanismos principales para cumplir esta tarea:

- **Segmentación:** Cuando, por ejemplo, se descarga un archivo MP3 de su sitio favorito de música, se está tratando con un bloque grande de datos. Con el fin de obtener este archivo desde el sitio de música hasta su PC, se necesita fragmentar en bloques más pequeños y manejables, para que la red lo pueda manejar. Este proceso se llama segmentación y la capa de transporte realiza esta función.
- **Direccionamiento de servicios:** Los protocolos de red (TCP/IP, por ejemplo) proporcionan diversos servicios de red y estos servicios se identifican por medio de puertos. La capa de transporte asegura que cuando los datos atraviesen la red, se pasen al servicio correcto y al puerto adecuado.
- **Revisión de error:** Los protocolos de la capa de transporte también realizan la revisión de error en los datos y aseguran que la información se envíe y reciba correctamente.

- Los protocolos que verá operando en la capa de transporte son de dos tipos:
- **Conexión orientada:** Un protocolo de conexión orientada (como el Protocolo de Control de Transmisión [TCP] requiere una conexión de extremo a extremo entre los servidores antes que se puedan transmitir los datos. Puede pensar en esto como en una llamada telefónica. Cuando se hace una llamada, no se puede comenzar a hablar con la persona al otro extremo de la línea hasta que se conecte exitosamente con esa persona.
- **Sin conexión:** Un protocolo sin conexión (como el Protocolo de Datagrama de Usuario [UDP]) permite la transmisión de datos sin requerir que se establezca una conexión. Los protocolos sin conexión se basan en la red para asegurar la entrega adecuada de datos de un servidor a otro. Se puede pensar en un protocolo sin conexión como al enviar un correo electrónico. Obviamente, no tiene que conectarse directamente con el receptor antes de enviar el correo; en vez de eso, escribe y pone la dirección en el mensaje, luego da clic en enviar. Aquí, aún puede confíar en la red (y no en una conexión existente) para asegurar que el correo llegue al destinatario.

La capa de transporte tiene una responsabilidad adicional en el modelo OSI: manejar el control de flujo de datos. El control de flujo determina cómo el dispositivo receptor acepta las transmisiones de datos. Existen dos métodos comunes de control de flujo:

- **Buffering:** El control de flujo de buffering almacena datos en un buffer y espera que el dispositivo del destino esté disponible. El buffering puede ser problemático si el dispositivo emisor está disponible para transmitir datos mucho más rápido que el dispositivo receptor disponible para recibirlos. Una velocidad de transmisión muy rápida puede sobrecargar un buffer, que tiene un tamaño limitado, causando pérdida de datos.
- **Ventana:** En un entorno de ventanas, se agrupan los segmentos de datos juntos y, cuando se envían, adquieren una sola aceptación. Aquí, los dispositivos de envío y recepción determinan el tamaño de la ventana (es decir, el número de segmentos que se puede enviar en una vez). En algunos casos, se determina el tamaño de la ventana cuando la conexión se establece; en otros, el tamaño de la ventana se basa en la congestión de la red y los recursos del dispositivo. Estos tipos de ventanas se conocen como ventanas deslizantes. Las ventanas mejoran el desempeño de la red, disminuyendo el número de aceptaciones que se necesita enviar entre los dispositivos.

★ Tome nota

Si está familiarizado con el hardware de las PC, tal vez reconoce estos dos métodos de control de flujo. Son los mismos métodos utilizados para el control de flujo en una PC cuando se mueven datos dentro y fuera de los diferentes tipos de almacenamientos de datos, incluyendo discos duros, caché y RAM

Capa de sesión (capa 5)

La capa de sesión es responsable de la sincronización de datos entre las aplicaciones en el dispositivo de envío y el dispositivo de recepción. Esta capa establece, mantiene y fragmenta sesiones entre los dos dispositivos. Mientras que la capa de transporte es responsable de las conexiones entre los dos dispositivos, realmente es la capa de sesión la responsable de transferir datos entre los dos dispositivos.

Capa de presentación (capa 6)

La capa de presentación convierte los datos de capa de la aplicación en un formato que se pueda transmitir a través de la red. Los datos formateados para el transporte a través de la red no siempre son legibles para las aplicaciones. Algunos formatos comunes de datos que son convertidos por la capa de presentación incluyen los siguientes:

- Archivos de gráficos

- Archivos de datos y texto
- Archivos de video y música

La capa de presentación es también en la que se realiza el cifrado y descifrado de datos.

Capa de aplicación (capa 7)

Finalmente, en la cima del modelo OSI está la capa de aplicación. Esta capa toma los datos del usuario y los pasa a las capas inferiores del modelo OSI para trasportarlos. Las respuestas son pasadas a través de las capas y mostradas al usuario.

Tome nota

Es importante recordar que la capa de aplicación del modelo OSI es no es la aplicación actual que se ve en la computadora. Más bien, se utiliza para definir cómo las aplicaciones que corren en la computadora pueden tomar ventaja del servicio de red. Por ejemplo, si quiere imprimir un documento en una impresora de red, su aplicación de procesamiento de palabras tomaría la información del archivo y la pasaría a la capa de aplicación, la cual luego la mandaría a las otras capas en el modelo, de manera que podría transmitirse a la impresora. Por supuesto, hay aplicaciones (programas de software) que tal vez podrían utilizar la aplicación o servicio de red que se ejecuta en los servicios de la capa de aplicación, como los navegadores web

Aunque el modelo OSI proporciona un marco para clasificar la tecnología, este modelo no se implementa totalmente en las redes de hoy en día. En vez de eso, las redes de la actualidad siguen un modelo simplificado que consta generalmente de las siguientes cuatro capas:

- **Capa de enlace:** Ésta es la capa más baja del modelo TCP/IP y está diseñada para ser hardware independiente. Es responsable de enlazar con la tecnología de red de hardware y transmitir los datos. EL TCP/IP ha sido implementado prácticamente en toda tecnología de hardware de redes existente hoy en día.
- **Capa de Internet:** Esta capa es responsable de conectar las redes múltiples y enrutar los paquetes entre ellas.
- **Capa de transporte:** Esta capa es responsable de que el mensaje de extremo a extremo transfiera las capacidades independientes de la red subyacente. También maneja el control de errores, segmentación, control de flujo, control de congestión y direccionamiento de aplicaciones (número de puertos).
- **Capa de aplicación:** El término "capa de aplicación" se refiere a los servicios y protocolos de red de alto nivel, tales como SMTP o FTP.

Ahora que comprende el modelo OSI, se pueden discutir diversas tecnologías de redes y el impacto en su programa de seguridad de información.

▶ *Análisis de Firewalls de Hardware y sus Características*

En el ambiente actual de redes, la gran mayoría de producción de cortafuegos se basa en el hardware. Es un firewall que se ejecuta en una plataforma dedicada, específicamente diseñada, optimizada y endurecida (el proceso de asegurar un sistema) para ejecutar un software de la aplicación.

Aunque hay una variedad de tipos de cortafuegos, cada uno con características diferentes, todos comparten algunas funciones básicas. Una es, que todo el tráfico de filtro se basaba en

un conjunto de reglas configuradas. Generalmente, estas reglas se basaban en información contenida en los paquetes de datos que viajan a través de la red. En particular, la información que encabeza el paquete de esos datos proporciona a los cortafuegos la información que necesitan para aplicar adecuadamente las reglas. Estas reglas generalmente son definidas por las políticas de seguridad de la compañía y los requisitos empresariales.

★ Tome nota

No se retrase mucho con las definiciones de tipos de cortafuegos. En vez de eso, busque comprender la funcionalidad de cada uno. Conocer los diferentes tipos no es tan importante como conocer cómo funcionan

Aunque es posible configurarlos para permitir todo el tráfico y sólo bloquear tráfico específicos basado en reglas, virtualmente todos los cortafuegos trabajan de acuerdo con la filosofía rechaza todo, permite lo específico. Esto significa que el firewall, por default, rechazará todo el tráfico, de manera que todo el que está permitido para atravesarlo debe ser configurado explícitamente en las reglas de firewall.

Hay una variedad de tipos de firewall y, dependiendo quién lo define, tal vez podría incluso encontrar que diferentes personas definen los tipos de firewall de maneras diversas. La clave es comprender los principios básicos, ya que, fuera de aprobar la prueba de certificación, generalmente no se le pedirá identificar tipos de firewall en sus deberes diarios.

Análisis del filtrado de paquetes

El primer tipo de cortafuegos es conocido como de filtrado de paquetes. Esta clase se considera de primera generación, ya que los primeros funcionaban como filtros de paquetes. Como se señala, el propósito primordial de un cortafuegos es filtrar el tráfico. Por consiguiente, y como sugiere el nombre, un cortafuegos de filtrado de paquetes inspecciona los paquetes de datos que intentan atravesarlo y se basa en las reglas que se han definido en el firewall, este permite o niega cada paquete conforme es adecuado.

Una de las primeras versiones de este tipo de firewall fue el router de filtrado de paquetes. Los routers tienen la capacidad de hacer algunos filtrados rudimentarios, tales como permitir todo el tráfico de salida mientras rechaza todo el tráfico entrante, o de bloquear el paso de los protocolos específicos a través del router, tales como telnet o ftp.

A diferencia de los routers, los cortafuegos mejoran el filtrado de paquetes, aumentando el control granular. Por ejemplo: tal vez configure uno de estos firewalls para bloquear el navegador web en Internet excepto el sitio web de su compañía, mientras que, al mismo tiempo, permite la salida de tráfico web de su red interna hacia Internet. O quizá podría establecer una regla que suprima todas las solicitudes de ping a menos que se originen en la estación de trabajo de un miembro del equipo de la red.

Cuando configura una regla de cortafuegos de filtrado de paquetes, generalmente utilizará uno o más de los siguientes atributos TCP/IP:

- Direcciones IP de origen
- Direcciones IP de destino
- Protocolo IP (telnet, ftp, http, https, etc.)
- TCP de origen y puertos UDP (por ejemplo: el protocolo http se ejecuta en el puerto 80 TCP)
- TCP de destino y puertos UDP
- La interfaz de red de cortafuegos entrante
- La interfaz de red de cortafuegos saliente

Algunos de los puertos y protocolos más comunes que encontrará en una red de producción incluyen los siguientes:

- FTP (transferencia de archivo) 20/tcp y 21/tcp
- Telnet (acceso a terminal) 23/tcp
- DNS 53/udp y 53/tcp
- HTTP (web) 80/tcp
- HTTPS (web) 443/tcp
- SMTP (correo electrónico) 25/tcp
- POP3 (correo electrónico) 110/tcp
- IMAP3 (correo electrónico) 220/tcp
- IMAP4 (correo electrónico) 143/tcp
- LDAP (servicios de directorio) 389/tcp
- Servidor SQL 1433/tcp
- RDP (servicios de terminal) 3389/tcp

Ésta no es una lista íntegra, ya que hay miles de protocolos y puertos diferentes, pero éstos son los más comunes que verá cuando configure las reglas en un firewall de filtrado de paquete. Para una lista completa de los protocolos y puertos, visite http://www.iana.org/assignments/port-numbers.

Análisis de los cortafuegos a nivel de circuito

Los ***cortafuegos a nivel de circuito*** se consideran típicamente como una tecnología firewall de segunda generación. Funcionan de modo similar a los de filtrado de paquetes, pero operan en las capas de sesión y transporte del modelo OSI.

En vez de analizar cada paquete individual, monitorea a nivel de circuito las sesiones TCP/IP, observando el protocolo de intercambio entre los paquetes para validar la sesión. El tráfico se filtra basado en las reglas de sesión específicas y podría restringirse sólo a computadoras autorizadas. Cuando se establece la sesión, el cortafuegos mantiene una tabla de conexiones válidas y permite el paso de datos cuando la información de la sesión corresponde con una entrada de la tabla. Cuando se finaliza la sesión, se extrae la entrada de la tabla y se cierra el circuito. Una característica única de los cortafuegos a nivel de circuito es que las sesiones que cruzan este tipo parecen originarse en el mismo. Esto permite que se oculte la red interna de la red pública.

Un cortafuegos a nivel de circuito también se conoce como proxy transparente, porque (como se mencionó) todas las sesiones parecen originarse ahí mismo. Casi siempre se utilizan en conjunto con otros tipos de cortafuegos, ya que sólo están disponibles para permitir las sesiones de las computadoras autorizadas. La granularidad adicional se requiere típicamente en la mayoría de los entornos de producción.

Análisis de los cortafuegos a nivel de aplicación

Los ***firewalls a nivel de aplicación*** (también conocidos como proxy) trabajan realizando una inspección profunda de los datos de la aplicación cuando atraviesan el cortafuegos. Se establecen las reglas analizando las peticiones del cliente y las respuestas de la aplicación,

luego, reforzando el comportamiento correcto de la aplicación. Estos cortafuegos pueden bloquear actividad malintencionada, registrar actividad del usuario, proporcionar filtrado de contenido e incluso proteger contra spam y virus. Microsoft Internet Security and Acceleration Server es un ejemplo.

Ahora para desventaja (la inspección profunda de los datos de la aplicación es un recurso) la actividad intensa y la potencia de procesamiento significativo quizá podría requerir disminuir las oportunidades de que impactará negativamente en el desempeño de la red. Cuanto más profunda sea la inspección, mayores son los requisitos de la fuente y mayor la posibilidad de un efecto perjudicial. Por lo tanto, cuando se despliega un cortafuegos a nivel de la aplicación, es importante que se estime adecuadamente. Simplificar los procesadores y RAM en el cortafuegos a nivel de aplicación es una fórmula excelente para originar usuarios molestos, y siempre es mejor idea tener un poco más poder que las necesidades inmediatas. Recuerde planear siempre para crecer. El uso de la red pocas veces disminuye con el paso del tiempo. Generalmente, no se quiere regresar a la gestión en un año para consolidar una actualización.

Una capacidad disponible en algún cortafuegos a nivel de aplicación que pueda compensar los efectos del desempeño negativo de la inspección profunda es la adición del almacenamiento en caché. Almacenar en caché permite que guarde datos descargados frecuentemente y los proporcione en respuesta a las peticiones de un usuario en vez de tener que recuperar los datos de Internet. La mayoría de los navegadores web tienen esta capacidad para el almacenamiento local de páginas utilizadas frecuentemente; un cortafuegos de almacenamiento en caché extiende esta capacidad para todos los usuarios en la red. Por ejemplo: si cincuenta empleados leen la primera página de la versión en línea de Wall Street Journal cuando llegan a la oficina, el cortafuegos almacenará en caché la primera visita al sitio, luego atenderá la página almacenada para los siguientes cuarenta y nueve visitantes.

El almacenamiento en caché era una tecnología mucho más eficiente durante los primeros días de Internet, cuando la mayoría del contenido era estático. En años recientes, con la llegada de las vistas adaptables al cliente, los mashups y el contenido interactivo, la eficiencia del almacenamiento en caché se ha vuelto más y más limitada.

Análisis de los cortafuegos con estado Multinivel

Los ***cortafuegos con estado Multinivel*** están diseñados para proporcionar las mejores características tanto de los cortafuegos a nivel de aplicación como de filtrado de paquetes. Este tipo provee un filtrado de paquete a nivel de red y también es capaz de reconocer y procesar los datos a nivel de aplicación. Cuando se configura correctamente, estos pueden proporcionar el nivel más alto de seguridad de todos los tipos de cortafuegos discutidos aquí; sin embargo, generalmente son los más caros. Además, con todas sus características disponibles, también pueden ser muy complejos para configurar y mantener.

▶ *Cortafuegos de hardware contra cortafuegos de software*

Antes de que consideremos cuándo es adecuado utilizar un cortafuegos de hardware en vez de uno de software, se necesita revisar qué quiere decir este término Hay dos tipos básicos:

- ***Cortafuegos del host:*** Este tipo de cortafuegos de software se instala en un host y se utiliza para protegerlo de los ataques basados en la red. Un ejemplo de este tipo de aplicación es el cortafuegos de Windows, incluido en versiones recientes de los sistemas operativos Microsoft. También se conocen como cortafuegos personales.

- ***Cortafuegos de red***: Esta categoría de cortafuegos de software consta de aplicaciones que se instalan en servidores utilizados para proteger los segmentos de red de otros. Estos tipos ofrecen una funcionalidad similar a la de los cortafuegos de hardware. Los más populares son aquéllos producidos por Cisco.

La única circunstancia en la cual claramente no tiene sentido utilizar un cortafuegos de hardware es para proteger un solo servidor. Si se necesita proteger un solo servidor, la mejor solución es instalar uno de software en él con un conjunto específico de reglas basadas en qué se está intentando proteger. Si el servidor es parte de una red más grande, que casi siempre es el caso, entonces cualquier firewall de red desplegado en la red también protegerá el host.

Aparte de los cortafuegos del host, hay una variedad de factores que impactarán la decisión de utilizar o no una solución de software o hardware para proteger su red. Muchos de estos factores se relacionan con algunos de los desafíos asociados con los cortafuegos de software. Los cuales incluyen los siguientes:

- **Hardware de host:** Los cortafuegos de software se ejecutan en el hardware de propósito general del servidor. Esto puede general cuellos de botella (incluyendo cuellos de botella de la red, memoria o procesador), especialmente si el hardware no está calculado adecuadamente para dirigir los requisitos de tráfico relacionados con el funcionamiento de una aplicación.
- **Sistema operativo del host:** Aunque tanto los cortafuegos del hardware como del software ejecutan sistemas operativos, el de hardware ejecuta uno endurecido, que proporciona una superficie de ataque más pequeña que uno débil. Con el fin de que coincida el nivel de seguridad del sistema operativo endurecido proporcionado por uno de hardware, un servidor de cortafuegos de software debe endurecerse igualmente. Esto puede requerir experiencia especializada e inversiones adicionales tanto en tiempo como en recursos. Como resultado, la mayoría de los firewalls de software tienen superficies de ataque más grandes que sus homólogos de hardware.
- **Otras aplicaciones:** Los cortafuegos de software deben competir por los recursos con otros procesos que se ejecutan en el host. En contraste, uno de hardware dedica sus recursos, estos no se comparten con ningún otro servicio. Como resultado, cuando se utiliza un cortafuegos de software, tal vez podría darse cuenta que necesita de hardware adicional para que corresponda el desempeño del mismo, debido a los requisitos de recursos adicionados.
- **Disponibilidad/estabilidad:** Un tema potencial relacionado con el uso de cortafuegos de software es que la confiabilidad se relaciona con la del hardware asociado y el sistema operativo subyacente. Aunque los componentes del hardware en un host generalmente serán tan confiables como los componentes en un cortafuegos de hardware, no siempre están disponibles en una configuración redundante, como lo están los de hardware. Los sistemas operativos han tenido un gran avance en términos de estabilidad, pero uno de propósito general tal como se utilizaría con un cortafuegos de software típicamente no es tan estable como el sistema operativo utilizado en un cortafuegos de hardware.

A pesar de los desafíos asociados con los cortafuegos de software, aún hay un par de razones convincentes para utilizarlos. Primera, son muy redituables. Segunda, por lo general son menos complejos para instalar y darles soporte técnico que sus homólogos de hardware.

Por consiguiente, en un entorno de red mediana a grande en la cual el desempeño, disponibilidad y confiabilidad son críticas, un cortafuegos de este tipo es la mejor solución. Es más, hallará algunos de hardware prácticamente en todas las redes de la empresa. En contraste, si tiene una red pequeña, y está intentando mantener costos bajos o asegurar un solo host, entonces utilizar uno de software podría ser la respuesta correcta.

Inspección Stateful contra la Inspección Stateless

Como se discutió antes, la mayoría de los sistemas de cortafuegos más básicos trabajan filtrando paquetes. Un cortafuegos de filtrado de paquetes inspecciona los paquetes de datos que intentan atravesarlo, basado en las reglas que se han definido en él, permite o niega cada paquete. No considera ninguna otra información relacionada con los paquetes cuando determina cuáles deja atravesar el firewall y cuáles no. Este tipo de inspección de paquetes de datos se conoce como inspección stateless.

En la inspección stateless, los datos que atraviesan el cortafuegos son examinados en busca de información como la siguiente:

- La dirección IP del dispositivo emisor
- La dirección IP del dispositivo receptor
- El tipo de paquete (TCP, UDP, etc.)
- El número de puerto

La inspección Stateful lleva el filtrado de paquetes al siguiente nivel. Además de examinar la información que encabeza los paquetes que atraviesan el firewall, una inspección stateful considera otros factores al determinar si se debería permitir o no el paso al tráfico a través del firewall. La inspección stateful también determina si un paquete es o no parte de una sesión existente y qué información se puede utilizar para decidir si se permite o niega el paso de un paquete. La sesión existente se conoce como el estado, que ocurre con frecuencia en la capa 4 (la capa de transporte) del modelo OSI. Muchos de los firewalls de inspección stateful actuales también pueden rastrear las comunicaciones a través de las capas 5 a 7.

La inspección stateful quizá sonaría relativamente fácil, pero en realidad es un proceso muy complejo, que es por lo que los firewalls de inspección stateful típicamente son más costosos y desafiantes para configurar. Un firewall de inspección stateful mantiene el rastro de todas las sesiones actuales en una tabla de estado almacenada en la memoria. En otras palabras, cuando se inicia una conexión al sitio web de MSN para revisar los titulares de hoy, el firewall almacena la información respecto a su sesión en una tabla. Lo mismo ocurre con todas las conexiones que suceden a través de firewall. Entonces, como cada paquete llega al firewall, se analiza para determinar si es parte de una sesión existente (estado). Si lo es, y si la sesión se permite con base en las reglas actuales del firewall, entonces pasa el paquete. En contraste, si el paquete no es parte de una sesión existente y no se utiliza para iniciar una sesión permitida, se desecha.

Otro beneficio de la inspección stateful es que una vez que se establece una sesión, el firewall gestiona el acceso con base en las sesiones en vez de los paquetes. Esto permite un conjunto más simple de reglas de firewall cuando se compara con los firewalls tradicionales de filtrado de paquetes. Un firewall de filtrado de paquetes requiere una regla para cada paquete autorizado. Por lo tanto, si se quiere permitir una conexión entre el Host A y Host B a través del firewall de filtrado de paquetes, se necesita una regla que permita los paquetes del Host A al Host B, así como otra regla que permita los paquetes del Host B al Host A. En comparación, cuando se utiliza el firewall stateful, se puede definir una regla que permita una conexión del Host A al Host B y entonces la gestión de la tabla de estado del firewall permitirá automáticamente el tráfico de regreso.

Los firewalls stateful hacen excelentes firewalls de perímetro para proteger una red interna de Internet, para proteger los host basados en zonas desmilitarizadas (discutidas con mayor detalle posteriormente en esta lección) de Internet y para proteger las extranets de las conexiones de clientes, proveedores o socios comerciales.

▪ Controlar el acceso con la Protección de Acceso a Redes (NAP)

↓ EN RESUMEN

Uno de los problemas con los que muchos programas de seguridad luchan es cómo asegurar que las computadoras conectadas a la red cumplan con las políticas de seguridad de la organización. Las compañías quieren estar seguras de que todas las computadoras tienen todos los parches, que ejecuten un software de antivirus actualizado y que pertenezcan a la organización antes de permitirles conectarse a la red. El desafío es hallar un mecanismo que permita que la red revise todos los sistemas antes de conectarse. Como solución a este problema, Microsoft ha desarrollado Network Access Protection como parte de Windows Server 2008.

☑ Listo para la Certificación

¿Cómo puede estar seguro que todas las computadoras de la red tienen un paquete de antivirus actualizado y los parches de seguridad vigentes de Microsoft? —3.2

Reconociendo la necesidad que los administradores deben tener más control gradual sobre qué sistemas se conectan a una red, Microsoft introdujo ***La Protección de Acceso a Redes (NAP)*** como parte del sistema operativo Windows Server 2008. La NAP es una solución que permite a los administradores tener una manera más eficiente de controlar el acceso a los recursos de la red. Los controles de la NAP se basan en la identidad de la computadora del cliente y si la computadora cumple o no con las políticas obligatorias de la red configurada.

La NAP es un conjunto complejo de controles, siendo una discusión completa que podría llenar fácilmente esta lección entera o incluso este libro. Por lo tanto, para los propósitos de esta sección, sólo examinaremos la NAP en el nivel más alto, discutiendo su finalidad, componentes y requisitos.

► *El propósito de la NAP*

La NAP permite a los administradores de la red definir los niveles graduales más altos de acceso a ésta, basados en quién es el cliente, a qué grupos pertenece y cómo cumple con base en la política de la NAP. Si un cliente no cumple, la NAP proporciona un mecanismo para hacer automáticamente que éste cumpla. Entonces, una vez que el cliente cumple y todos los problemas se han corregido, la NAP dinámicamente aumentará el nivel del cliente para el acceso a la red.

★ Tome nota

Si va a implementar la NAP en su entorno, asegúrese de invertir algo de tiempo al ejecutarlo en modo monitor. Esto le permitirá obtener una mejor comprensión del impacto de la política de acceso limitado si se implementa o cuando lo haga. Aunque la seguridad es importante, es una buena idea extender nuevas capacidades de seguridad con el menor impacto posible a los usuarios

La NAP tiene tres componentes distintos:

- **Validación del estado de salud:** Con el fin de que la NAP valide el estado de salud de una computadora, el administrador primero debe definir las políticas de requisitos de salud. Luego, cuando la computadora intenta conectarse a la red, los system health agents (SHA) y los system health validators(SHVs) confirman la su configuración con la política de requisitos de salud. Además de definir estas políticas, los administradores también deben definir qué acción tomar si una computadora no cumple con los requisitos. La NAP puede configurarse sólo para monitorear; de esta manera los resultados de la revisión de salud del sistema se registran para un análisis posterior. Si la NAP se configura para acceso limitado, las computadoras que no cumplan las políticas de requisito de salud tendrán un acceso limitado a la red restringida. Por lo general, esto implicaría el acceso a un servidor de recuperación, para que se puedan corregir los problemas de la computadora. En contraste, las que obedezcan las políticas de requisito de salud se les concederá acceso ilimitado a la red.
- **Cumplimiento con las políticas de salud:** Los administradores pueden garantizar este requisito con el cumplimiento de las políticas de salud, configurando la NAP

para actualizaciones automáticas en las computadoras que no cumplan con los cambios de configuración o la falta de actualizaciones de software. Es importante comprender que estos cambios para cumplir con los requisitos se realizan utilizando el software de gestión de configuración, no a la NAP originalmente. Cuando la NAP se configura sólo para monitorear, las computadoras que no cumplen tienen acceso a la red, de manera que pueden actualizarse con los cambios de configuraciones o actualizaciones requeridas. En comparación, cuando la NAP se configura en modo de acceso limitado, las computadoras que no cumplen tienen un acceso limitado hasta que éstas cumplan con los cambios de configuración y actualizaciones requeridas. En este caso, los recursos requeridos para actualizar el sistema deberían incluirse en las partes de la red que pueden accesar a la computadora. Ya sea que se configure la NAP en acceso limitado o de monitoreo, se puede hacer que todas las computadoras compatibles con la NAP cumplan automáticamente. Para las computadoras que no pueden admitir la NAP (versiones anteriores de Windows, sistemas operativos que no son Windows, etc.), los administradores pueden definir excepciones que aún puedan permitir el acceso a la red.

- **Modo de acceso limitado:** El componente final que la NAP proporciona para proteger una red es el modo de acceso limitado. Este modo permite a los administradores proteger sus redes, limitando el acceso de las computadoras que no cumplen. Estas computadoras se pueden limitar en base al tiempo (qué tanto tiempo están conectadas) o a qué partes de la red pueden acceder. Si se configura con acceso limitado, se recomienda que este acceso incluya los recursos necesarios para el cumplimiento de la computadora. Entonces, después de que la computadora cumple, la NAP puede abrir su acceso de manera dinámica, sin necesidad de reiniciar o re-autenticación.

Cómo funciona la NAP

Existe una variedad de componentes utilizados para hacer que funcione la NAP, incluyendo los system health agents (SHA) y los system health validators (SHV). Los SHA se ejecutan en la computadora del cliente y reportan el estatus de la misma a los SHV, que se están ejecutando en la red y gestionan la configuración de la NAP.

Estos componentes proporcionan el rastreo del estado de salud y la validación del cumplimiento. Ellos son la base del servicio de la NAP, ya que permiten que ésta determine qué acción debe realizarse con base en la configuración de la computadora.

Los sistemas operativos del cliente que tienen un Windows Security Health Validator SHA para monitorear los ajustes del Windows Security Center incluyen los siguientes:

- Windows Vista Business
- Windows Vista Enterprise
- Windows Vista Ultimate
- Windows 7 Home Premium
- Windows 7 Professional
- Windows 7 Ultimate
- Windows XP Service Pack 3

Windows Server 2008 incluye su correspondiente Windows Security Health Validator SHV. Aunque actualmente está muy influenciado por Microsoft, la NAP es extensible y tiene un API que permite a cualquier vendedor proveer sus propios SHA y SHV para interoperar con la NAP.

La otra parte importante del rompecabezas de la NAP es la pieza de ejecución. Con la NAP, los enforcement client (EC) y enforcement servers (ESs) realizan esta función. Estos componentes necesitan la validación del estado de salud y, si una computadora no cumple con los requisitos, éstos ejecutan un acceso limitado a la red utilizando el Network Policy Server (NPS), que es un componente en Windows Server 2008.

El NPS es el servidor RADIUS (Remote Authentication Dial-In User Service) y el servicio proxy en Windows Server 2008. Cuando el NPS funciona como un servidor RADIUS, éste proporciona servicios de Autenticación, Autorización y Auditoría (AAA) para el acceso a la red. Cuando se utiliza la autenticación y autorización, y una computadora intenta una conexión autentificada de 802.1x o una conexión VPN, el NPS interactúa con el Directorio activo para verificar las credenciales de la computadora o usuario, así como para obtener sus respectivas propiedades de cuenta.

El NPS también actúa como un servidor de políticas de salud de la NAP. En particular, los administradores definen los requisitos de salud del sistema como parte de las políticas de salud del servidor NPS siendo así como el servidor evalúa la información del estado de salud proporcionado por los clientes de la NAP para determinar si los éstos cumplen o no con ellos. Cuando se determina que un cliente no cumple con los requisitos, el servidor NPS ofrece un conjunto de acciones de corrección que el cliente de la NAP debe llevar a cabo para cumplir.

El papel del NPS como un servidor AAA es independiente de su función como un servidor de políticas de salud de la NAP. Estas funciones se pueden utilizar de manera separada o combinada, según sea necesario.

El NPS también permite actuar a Windows Server 2008 como servidor de políticas de salud, ejecutando el acceso limitado de las siguientes maneras:

- **Ejecución IPsec:** La ejecución IPsec requiere que el cliente que se está conectando sea configurado para ejecutarla antes de que pueda conectarse con otros hosts. Éste es el más estricto de los diversos mecanismos de acceso limitado, ya que la computadora del cliente no puede comunicarse con otra computadora hasta que se configuren las comunicaciones de la IPsec. La ejecución de la IPsec permite cumplir cualquier aspecto para el cual se configure el cliente de Windows IPsec. Puede requerir de comunicaciones con otras computadoras actualizadas en una dirección IP o por un número de puerto base. Ésta es una configuración muy segura, debido al hecho de que encripta todos los datos que atraviesan la red. De hecho, rara vez se verá la configuración de la NAP, a menos que esté trabajando en un ambiente de seguridad muy alto que encripte todo el tráfico de la red.
- **Ejecución 802.1x:** La ejecución 802.1x requiere que el cliente de la conexión cumpla para obtener el acceso completo a través de una conexión de red autentificada 802.1x. Aquí, el cliente no sólo debe ser capaz de autenticarse exitosamente utilizando 802.1x, también debe cumplir la política de salud activa. La política de salud se ejecuta cada vez que el cliente intenta conectarse con la red y se autentifica con 802.1x. Para las computadoras que no cumplen las políticas, el acceso a la red es limitado por medio de un perfil de acceso restringido en el dispositivo de la red. El perfil restringido puede especificar los filtros del paquete o forzar a la computadora para unirse a una VLAN restringida. Es importante recordar que la ejecución 802.1x también monitoreará activamente el estatus de salud del cliente conectado y, si el cliente no cumple las políticas, se aplicaría el perfil de acceso restringido a la conexión.

Tome nota

El 802.1x es un protocolo de autentificación utilizado para asegurar las redes LAN de las conexiones del cliente. La autentificación 802.1x implica tres partes: un cliente (también conocido como el suplicante), un dispositivo de red (también conocido como el autentificador) y un servidor de autentificación. Cuando el cliente quiere conectarse a la red, se hace una petición al dispositivo de la red. Entonces, éste dispositivo remite esa petición al servidor de autentificación, utilizando el RADIUS. El servidor de autentificación a continuación determina si se permite el dispositivo del cliente en la red. Si es permitido, entonces el dispositivo de la red permite que se conecte

- **Ejecución VPN:** La ejecución VPN requiere que una computadora cumpla los requisitos con el fin de obtener acceso ilimitado a través de la conexión VPN de acceso remoto. Esto puede ser un gran beneficio para las organizaciones con gran número de empleados remotos. Uno de los principales retos que enfrenta una compañía con muchos usuarios remotos es asegurar que estas computadoras de los usuarios permanezcan con todos los parches, ejecutando un software antivirus actualizado y estén configuradas de manera segura. La NAP resuelve esta cuestión con la ejecución del VPN. Las computadoras que no cumplen los requisitos reciben el acceso restringido a la red por medio de los filtros de paquetes IP aplicados por el servidor VPN. Al igual que la ejecución 802.1x, la ejecución VPN hace respetar los requisitos de políticas de seguridad cada vez que la computadora intenta utilizar una conexión VPN de acceso remoto para conectarse a la red. La ejecución VPN también monitorea activamente el estatus de salud del cliente conectado y, si el cliente no cumple las normas, se aplicaría el perfil de acceso restringido a la conexión.
- **Ejecución DHCP:** La ejecución DHCP requiere que una computadora cumpla las políticas de salud con el fin de obtener una configuración de dirección IPv4 de acceso ilimitado de un servidor DHCP. Para las computadoras que no cumplan los requisitos, el acceso está limitado por una configuración de dirección IPv4 que permite el acceso sólo a una red restringida. La ejecución DHCP hace cumplir los requisitos de las políticas de seguridad cada vez que un cliente DHCP intenta descargar o renovar una configuración de dirección IP. Al igual que con los otros modos de acceso limitado, la ejecución DHCP también monitorea activamente el estatus de salud del cliente de la NAP y renueva la configuración de la dirección IPv4 sólo para accesar a la red restringida si el cliente no cumpliera con los requisitos.

El último elemento importante de la instalación de la NAP es el servidor de corrección. Estos servidores, que no son un componente formal de la NAP (no hay ningún acrónimo relacionado con los servidores de corrección), constan de servidores, servicios u otros recursos que una computadora que no cumple con los requisitos puede utilizarlos para cumplirlos. Por supuesto, para que una computadora que no cumpla las políticas utilice los servidores de corrección, éstos deben estar disponibles como parte del acceso limitado concedido a la computadora.

Un servidor de corrección tal vez podría contener las firmas de virus y actualizaciones de software más recientes, podría ser un servidor web que requiera credenciales de 802.1x o incluso podría ser un servidor web con instrucciones de cómo configurar la IPsec para conectarse a la red. La estructura de los servidores de corrección es específica para su entorno y sus políticas de salud. Un SHA puede comunicarse directamente con un servidor de corrección, o en su lugar, puede utilizar software instalado por el cliente para solucionar los problemas.

Requisitos para la NAP

Como se mencionó anteriormente, varios sistemas operativos de Microsoft soporten la NAP, incluyendo los siguientes:

- Windows Server 2008 o Windows Server 2008 R2
- Windows Vista Business
- Windows Vista Enterprise
- Windows Vista Ultimate
- Windows 7 Home Premium
- Windows 7 Professional
- Windows 7 Ultimate
- Windows XP Service Pack 3

Sin embargo, hay diversos componentes adicionales que podrían necesitarse con el fin de implementar exitosamente la NAP. Estos incluyen:

- Active Directory Domain Controller
- Active Directory-based Certificate Authority
- System Health Agents
- System Health Validators
- Servidor RADIUS
- Ejecución del cliente
- Ejecución del servidor
- Network Policy Server
- 802.1x network devices
- Servidor VPN
- Servidor DHCP
- Servidores de corrección

No todas las implementaciones de la NAP requerirán todos estos componentes, pero debe ser consciente de que quizá podría necesitarlos, dependiendo de por qué o cómo se está utilizando la NAP en la organización.

▪ Usar el aislamiento para proteger la red

↓ EN RESUMEN

Además de proteger el perímetro, puede utilizar diversas técnicas para proteger los recursos informáticos de la red interna. Estas tecnologías permiten aislar partes de la red, proporcionan un uso especial a los cortafuegos e incluso completar la seguridad proporcionada por éstos últimos. Los ruteos y VLAN son tecnologías de red que pueden ayudar a segregar la red en zonas de seguridad. Se puede implementar tecnologías como Honeypots para ayudar a distraer a los atacantes de las porciones importantes de la red y los cortafuegos también pueden desempeñar un papel si se necesita crear un DMZ en la red. Las VPN, las NAT, el aislamiento del servidor y el aislamiento del dominio son algunos conceptos adicionales que se pueden utilizar para asegurar la red.

▶ *LAN virtuales*

☑ Listo para la Certificación

¿Qué utilizaría para aislar la subred con todos sus servidores del resto de la red? —3.3

Antes de poder discutir qué es una LAN virtual, tenemos que revisar rápidamente el concepto de Red de área local (LAN). Es una red de servidores que cubren un área física muy pequeña, como una oficina, un piso de un edificio o un pequeño grupo de edificios. Las LAN se utilizan para conectar a varios hosts. Entonces, estas LAN se conectan con otras utilizando un router, que (como se discutió) es un dispositivo de capa 3.

Uno de los desafíos asociados con LAN es que a medida que éstas crecen, cada dispositivo transmite tráfico hacia ellas. Aunque estas transmisiones no atravesarán un router, si hay suficientes host, el tráfico total de las transmisiones puede saturar la red. Una solución es implementar más routers como una forma de dividir la red en segmentos más manejables. Sin embargo, los routers añaden latencia al tráfico de la red y requieren un protocolo de enrutamiento (discutido en la siguiente sección) para que el tráfico encuentre su camino de una parte de la red a otra.

Por consiguiente, las LAN virtuales (VLAN) fueron desarrolladas como una solución alternativa a la implementación de varios routers. Las VLAN son segmentos lógicos de red utilizados para crear dominios separados de transmisión, pero aún así permite que los dispositivos en la VLAN se comuniquen con la capa 2 sin necesidad de un router. Las VLAN se crean con interruptores, y el tráfico entre las VLAN se intercambia, no rutean, lo cual crea una conexión de red mucho más rápida, ya que no hay necesidad de involucrar el protocolo de enrutamiento. A pesar de que los hosts se separan de modo lógico, el tráfico entre estos se intercambia directamente como si el hosts estuviera en el mismo segmento de la LAN.

Las VLAN ofrecen una serie de beneficios a través de redes enrutadas, incluyendo los siguientes:

- Alto rendimiento en las LAN medianas o grandes, debido a que reduce la transmisión del tráfico.
- Una mejor organización de dispositivos en la red para facilitar su gestión.
- Seguridad adicional, ya que los dispositivos pueden colocarse en su propia VLAN.

Hay varias maneras diferentes de asignar hosts a las VLAN. Estos métodos son los siguientes:

- **Membresía VLAN por puerto:** Debido a que los puertos en un interruptor se definen al pertenecer a una VLAN específica, cualquier dispositivo que se conecte a un puerto es asignado a la VLAN correspondiente. Por ejemplo: un puerto con un interruptor treinta y dos podría tener los puertos 1-4 asignados a la VLAN1, los puertos 5-16 asignados a VLAN2 y los puertos 17-32 asignados

a VLAN3. Aunque parece un método sencillo para organizar los puertos, puede ser problemático si trabaja en un entorno en el cual los usuarios cambian frecuentemente sus ubicaciones en la oficina. Por ejemplo: si asigna puertos en una sección de cubículos para el departamento de ventas y, dos semanas después, la gerencia decide mover el departamento a otro lado del edificio, tendrá que configurar de nuevo el interruptor para soportar este movimiento. Sin embargo, en un entorno relativamente estable, este modelo funciona bien.

- **Membresía VLAN por dirección MAC:** Con este modelo, la membresía en una VLAN se basa en la dirección MAC del host. Cuando la VLAN se configura en el interruptor, los hosts se asignan con base en su dirección MAC. De este modo, cuando una estación de trabajo se cambia de ubicación y se conecta a un puerto de interruptor diferente, éste automáticamente asigna el host a la VLAN adecuada con base en la dirección MAC de la estación de trabajo. Debido a que la dirección MAC generalmente es *altamente codificada dentrodel host's NIC*; este modelo por lo general es más utilizado en un entorno en el cual se mueve el hosts. Una de las desventajas de este modelo es que requiere más trabajo inicial para instalarse, ya que se necesitan obtener todas las direcciones MAC de los hosts y asociarlas con las VLAN adecuadas.
- **Membresía por dirección de subred de IP:** En este tipo de asociación de VLAN, la membresía se basa en el elemento que encabeza la capa 3. El interruptor lee la dirección IP de capa 3 y asocia el alcance con la VLAN adecuada. A pesar de que el interruptor tiene acceso a la información de la capa 3 en el elemento que encabeza, la tarea de la VLAN se sigue haciendo en la capa 2 del modelo OSI y no se realiza ningún enrutamiento. Este modelo también es propicio para el entorno en el cual hay movimientos frecuentes del usuario. El desempeño podría ser afectado, debido a que el interruptor necesita leer el elemento que encabeza la capa 3 para determinar a qué VLAN se le asigna el hosts. Esto generalmente no es un problema con las tecnologías de los interruptores actuales, pero es bueno estar consciente de la sobrecarga adicional asociada a este modelo.
- **Membresía por protocolo:** Las VLAN también pueden ser organizadas en base al protocolo. Esto fue una solución útil cuando muchas LAN corrían múltiples protocolos de red, pero con el dominio actual de TCP/IP en prácticamente todas las redes, este modelo casi nunca se utiliza.

La siguiente pregunta que se debe pensar es: ¿Cómo ayudan las VLAN con la seguridad? En resumen, hay dos formas básicas para aprovechar una VLAN en apoyo a la seguridad.

Primero, debido a que la VLAN es una separación lógica, el tráfico en una no es directamente accesible a los hosts de otra. Sin embargo, esto es de uso mínimo, ya que ahora hay técnicas llamadas *VLAN hopping* que proporcionan acceso al tráfico en otras VLAN.

El segundo uso de la VLAN desde una perspectiva de seguridad es que permiten organizar mejor los hosts para asignar permisos de acceso. Esta técnica se utiliza en combinación con las listas de control de acceso o firewalls. Por ejemplo: si tiene una sección del edificio donde se sientan los administradores, puede crear una VLAN para esa área y proveer el acceso por medio de firewalls, de manera que estos empleados puedan acceder a todas las secciones de la red. Mientras tanto, el departamento de ventas podría estar en una VLAN que tenga acceso restringido a los servidores de aplicaciones de ventas, con acceso a finanzas y Recursos Humanos pero con las aplicaciones bloqueadas.

Qué es el enrutamiento

El enrutamiento se realiza en una etapa arriba del modelo OSI de una VLAN, en otras palabras, en la capa 3. Recuerde que el enrutamiento es el proceso de envío de un paquete basado en la dirección de destino del paquete. En cada etapa de la ruta del paquete a través de la red, se debe tomar una decisión respecto a dónde enviarlo. Para tomar estas decisiones, la capa de IP consulta la tabla de enrutamiento almacenada en la memoria del dispositivo de enrutamiento. Las entradas de la tabla de enrutamiento se crean por omisión cuando se inicia el TCP/IP y se agregan entradas adicionales ya sea de manera manual por el administrador del sistema o automáticamente por medio de la comunicación con los routers.

Sin embargo, ¿qué es exactamente un router? Previamente, se definió enrutamiento como el proceso de enviar un paquete con base en la dirección destino del éste. Por lo tanto, en su forma más simple, un router es cualquier dispositivo que envía paquetes de una interfaz a otra. Esta es una descripción muy simple para un proceso muy complicado.

Hay dos tipos básicos de router: software y hardware. Un router de software es una computadora que ejecuta un sistema operativo y múltiples servicios, incluyendo un servicio de enrutamiento. Por ejemplo: Windows Server 2008 soporta enrutamiento. Algunos de los beneficios de utilizar un enrutamiento de software son los siguientes:

- **La estrecha integración con el sistema operativo:** El servicio de enrutamiento se integra frecuentemente con el sistema operativo y otros servicios.
- **Interfaz de usuario compatible:** No se requiere nueva capacitación en un nuevo sistema operativo/interfaz: las funciones de enrutamiento se configuran mediante la interfaz estándar del usuario.
- **Bajo costo:** Si agrega el enrutamiento a un servidor existente, no debe pagar por el hardware dedicado. Esto disminuye el costo total, aunque si pensaba destinar un router de software para el enrutamiento, cualquier ahorro será insignificante.
- **Flexibilidad:** Los routers de software permiten configurar y ejecutar múltiples servicios en una sola plataforma.

¿Cuándo utilizar el router de software? Generalmente, encontrará el software del router en oficinas pequeñas que buscan soluciones fáciles de manejar que no son costosas. Otra circunstancia en la cual se podría utilizar un router de software es entre dos segmentos LAN donde se espera que sean bajos los requisitos de tráfico. Un ejemplo de esto podría ser un segmento de laboratorio donde se quiere aislar de los servidores de éste, pero no se desea invertir en un router de hardware.

Aunque hay beneficios al utilizar routers de software, también hay algunas desventajas importantes cuando se compara con routers de hardware. Estas incluyen las siguientes:

- **Bajo desempeño:** Debido a los gastos indirectos adicionales relacionados con el sistema operativo y cualquier otro servicio extra, los routers de software por lo general son más lentos que los de hardware.
- **Baja confiabilidad:** Cualquier router de software tiene el potencial para problemas con el sistema operativo y otros servicios que se ejecutan, así como para problemas con diversos componentes de hardware comparados con el router de hardware. Como resultado, son típicamente menos confiables que los de hardware.
- **Escalabilidad limitada:** Al escalar el router de software en múltiples interfaces de alta velocidad, se enfrentará a limitaciones del hardware de la computadora. Puesto que la mayoría de los servidores basados en la PC no están diseñados para enrutar múltiples tarjetas de interfaz en la red a alta velocidad, generalmente no escalan con facilidad o tanto como los de hardware. Así mismo, el añadir servicios como

listas de control de acceso o servicios de cortafuegos impactará el desempeño del router de software en mayor grado que uno de hardware compatible.

- **Admisión limitada del protocolo:** Los routers de software no soporten típicamente un número cercano a los protocolos de ruteo que un router de hardware acepta. Por ejemplo: Windows Server 2008 se limita al protocolo RIP de enrutamiento del IP y no soporta en ese momento ningún otro protocolo de enrutamiento más avanzado basado en el IP, como el BGP4.

Ahora se entiende qué implica un router de software, pero, ¿qué hay del router de hardware? Resumiendo, es un dispositivo de hardware dedicado cuya función principal es enrutar paquetes. Esta descripción no es tan precisa ahora como lo fue en años anteriores, no obstante, debido a que muchos de ellos son dispositivos multifuncionales (por ejemplo: pueden incluir, VPN, DHCP, firewall, almacenamiento en caché o, tal vez, incluso, servicios de detección de intrusión). Los beneficios en comparación con los routers de software incluyen los siguientes:

- **Alto desempeño:** Los routers de hardware corren en estas plataformas con un único propósito, con sistemas operativos y hardware altamente optimizados.
- **Alta confiabilidad:** Los routers de hardware son típicamente más confiables que sus homólogos de software, debido en gran parte a las capacidades limitadas del software en comparación con el hardware dedicado. Generalmente tienen mayor modularidad. También pueden utilizarse en pares, de manera que uno se activará si el otro falla. Aunque esto es teóricamente posible con un router de software, raras veces acontece.
- **Amplio soporte de protocolo de enrutamiento:** Los routers de hardware se pueden configurar para soportar cualquier protocolo, desde RIP a OSPF a BGP, siempre que adquieran las funciones adecuadas. También soportan un mayor número de algoritmos de enrutamiento que los routers de software. En un entorno más grande de red, podría ser crítico.

Como en otros aspectos, los routers de hardware tienen sus desventajas, incluyendo las siguientes:

- **Alto costo:** Típicamente, los routers de hardware son plataformas dedicadas, que por lo general las hace más costosas que los routers de software que también proporcionan otros servicios. Está línea es borrosa, ya que las características adicionales están disponibles en routers de hardware. Es decir, un router pequeño puede ser relativamente barato.
- **Poca simpatía con el usuario:** Por lo general, los routers de hardware se configuran utilizando una conexión Secure Shell y se gestionan por medio de una interfaz de línea de comando. Aunque hay herramientas gráficas para la gestión de routers, muchas configuraciones de éstos se realizan mediante la línea de comando que utilizan una lista extremadamente compleja de comandos. Por lo tanto, un ingeniero de soporte con experiencia puede configurar o mediar un router de hardware sin mucha dificultad, pero para alguien nuevo con los routers siempre habrá una curva de aprendizaje muy pronunciada.
- **Mayor complejidad:** Aunque un router de hardware individual podría no ser realmente mucho más complejo que su homólogo basado en software, cuando se escala en grandes redes, hace que un entorno de router de hardware puede convertirse rápidamente en una complicación extrema. Esta cuestión también podría aplicarse a los de software, pero estos no son tan comunes en el mundo real. En la mayoría de los entornos de redes, los de hardware se utilizan casi exclusivamente y los de software se reservan sólo para ubicaciones o redes pequeñas.

Cómo funciona el enrutamiento

Cuando un router recibe un paquete, debe reenviarlo al host del destino, entonces el debe tomar una decisión. En particular, necesita determinar si puede entregar el paquete directamente al host de destino o si necesita enviar el paquete a otro router. Para tomar esta decisión, examina la dirección de la red de destino. Si tiene una interfaz que se conecta con la misma red que el host de destino, puede entregar el paquete directamente. El asunto se vuelve interesante cuando el router no está conectado a la misma red que el host de destino: aquí, debe determinar la mejor ruta hacia el host de destino, para que pueda enviar correctamente el paquete.

★ Tome nota

Sólo porque hay una ruta al destino no significa que también haya una ruta de regreso. Aunque no es un problema común en las redes con enrutamiento dinámico habilitado, puede suceder particularmente si se trabaja en un entorno de red de cortafuegos muy pesado

Cuando un router necesita enviar un paquete a otro, utiliza la información de las tablas de enrutamiento para elegir el mejor camino para el paquete. Se determina a qué router se envía el paquete mediante diversas variables que pertenecen a la ruta de la red hacia del host de destino, incluyendo el numero de hops y el costo de cada uno, etc. Esta base de datos se almacena en la memoria del router para asegurar que el proceso de búsqueda se realice velozmente.

Cuando el paquete viaja a través de la red hacia su destino, cada router, a lo largo del camino toma una decisión respecto a dónde enviar el paquete al consultar su tabla de enrutamiento. Además, cuando el host de destino envía un paquete de respuesta, es posible que el paquete no pueda viajar de regreso al emisor original por la misma ruta. La ruta tomada por el paquete de respuesta depende de la métrica de cada trayectoria a lo largo de la ruta de regreso. En otras palabras, el camino al host de destino puede no ser el mejor camino de regreso hacia el host emisor.

Se puede generar la información de la tabla de enrutamiento de una de las dos formas. El primer método es configurar manualmente la tabla de enrutamiento con las rutas para cada red de destino. Esto se conoce como enrutamiento estático. El enrutamiento estático es más apropiado para los entornos pequeños en los cuales la cantidad de información para configurar es pequeña y los gastos indirectos de enrutamiento dinámico son inaceptables. Los routers estáticos no escalan bien las grandes redes o las que cambian frecuentemente, debido al requisito de gestión manual.

El segundo método para generar la información de la tabla de enrutamiento es utilizar un protocolo dinámico de enrutamiento. Debido a que los protocolos de enrutamiento dinámico son un poco más complejos que los de enrutamiento estático se necesita echar un vistazo más exhaustivo a este tema.

★ Tome nota

No lo olvide ¡Los routers también necesitan los parches! Pues debido a que ejecutan un sistema operativo, tienen actualizaciones de funcionalidad y seguridad que se deben aplicar

Una definición general de "protocolo" es un método acordado para intercambiar datos entre dos dispositivos. Por consiguiente, un protocolo de enrutamiento se define como el método para intercambiar la información de enrutamiento entre dos routers (y un protocolo de ruteo dinámico implica el intercambio de información de enrutamiento que se construye y mantiene automáticamente en una tabla de enrutamiento). En otras palabras, cuando se utiliza un protocolo de enrutamiento dinámico, la información se intercambia entre los routers y se utiliza para actualizar la información almacenada en cada tabla de enrutamiento del dispositivo. Esto se puede hacer periódicamente (en intervalos programados) o como se necesite. Si al principio se instalan correctamente, los routers dinámicos requieren poca gestión, fuera de asegurarse que las actualizaciones del software se apliquen a tiempo. Debido a que se enteran automáticamente de la información de enrutamiento y tienen la capacidad de enrutar alrededor de las fallas cuando la arquitectura de la red lo admite, los routers dinámicos se utilizan generalmente en el entorno de redes grandes en las cuales no sería práctico enrutar estáticamente.

Protocolos de enrutamiento

Los protocolos de enrutamiento se basan tanto en un vector a distancia como en un algoritmo de estado de enlace. Las diferencias entre los dos métodos se relacionan en el momento cuando se intercambia la información de enrutamiento, en qué información se envía durante este intercambio y qué tan rápido el protocolo puede enrutar alrededor de los cortes cuando la topología de la red los soporta. La selección de trayectoria implica aplicar una métrica de enrutamiento a las múltiples rutas para seleccionar la mejor. Algunas de las métricas utilizadas son el ancho de banda, la demora de red, el conteo de hop (concentrador), el costo de la trayectoria, carga, confiabilidad y costos de comunicación. (El conteo de hop es el número de routers atravesados por un paquete entre su origen y su destino).

Los protocolos de enrutamiento con base en el vector de distancia requieren que cada router informe a sus vecinos sobre su tabla de enrutamiento. Esto se realiza enviandola completa cuando arranca el router, y luego lo envía de nuevo a intervalos programados. Cada router toma las actualizaciones de (routers vecinos y luego actualiza su propia tabla de enrutamiento basado en esta información. Utilizando la información de estas actualizaciones, puede construir un mapa de la red en su tabla de enrutamiento y luego puede utilizar este mapa para determinar el conteo de hops para cada entrada de red. El RIP es un ejemplo de protocolo de enrutamiento con base en el vector a distancia que es admitido por Windows Server 2008.

Las actualizaciones de enrutamiento enviadas utilizando el protocolo de enrutamiento con base en el vector a distancia no son reconocidas ni sincronizadas, lo cual es una de las desventajas de estos protocolos. Algunas otras desventajas de este tipo de enrutamiento incluyen los siguientes:

- **Altos gastos indirectos:** Ya que cada router en la red envía su tabla de enrutamiento completa cuando manda una actualización, los protocolos de enrutamiento con base en el vector a distancia produce tablas muy grandes. Esto añade gastos indirectos a la memoria del router requerida para almacenar las tablas, así como el poder de procesamiento que tiene para mantenerlas. Las grandes tablas de enrutamiento también pueden dificultar las tareas de un administrador que intenta determinar el origen de un problema cuando éste surja.
- **Falta de escalabilidad:** Las redes con base en el vector a distancia se limitan a 15 hops (cruces del router) para cierta ruta. En una red grande (como Internet), es muy fácil tener segmentos de red que son más grandes que 15 hops (y tales segmentos estarían fuera del alcance en una red con base en el vector a distancia).
- **Utilización intensa de ancho de banda:** Los protocolos con base en el vector a distancia necesitan que los routers intercambien la tabla completa de enrutamiento cuando se actualizan. En una red grande con grandes tablas de enrutamiento, estas actualizaciones pueden utilizar cantidades importantes de ancho de banda, especialmente a través de conexiones WAN pequeñas, o por enlaces dial.
- **Tiempo de convergencia largo:** Las convergencias son la cantidad de tiempo que le toma a un algoritmo de enrutamiento el detectar y enrutar alrededor de una falla de la red. Los protocolos con base en el vector a distancia típicamente tienen tiempos de convergencia más largos que los protocolos con base en el estado de enlace (descritos a continuación en esta lección).
- **Problemas de Bucle de enrutamiento (o ciclo de enrutamiento):** Los protocolos con base en el vector a distancia también pueden sufrir problemas de Bucle de enrutamiento cuando hay trayectorias múltiples hacia una red. Es cuando un paquete se envía o regresa entre dos redes o a través de múltiples redes donde el paquete, finalmente, se envía de regreso a la red que lo mandó. Ya que es un bucle, el paquete nunca llega a su destino. Si uno o más mecanismos no están en posición

para lidiar con estos y los paquetes que están atrapados en él no son entregados, la red podría congestionarse eventualmente, ya que se encarga de los paquetes perdidos.

- **Problema de la cuenta a infinito:** El problema de la cuenta a infinito sucede cuando hay un corte de red y el algoritmo de enrutamiento no puede calcular un nuevo router. Aquí, un router transmitirá una ruta y aumentará el conteo de hop, luego el segundo router transmitirá la misma ruta al primer router, también incrementando el conteo de hop, así sucesivamente, hasta que el enrutado métrico (conteo de hop) llegue a 16 y la ruta se deseche.

Afortunadamente, algunos protocolos de enrutamiento con base en el protocolo de vector a distancia tienen mecanismos adicionales que les permiten evitar el problema de la cuenta a infinito, así como a mejorar la convergencia. Estos mecanismos son los siguientes:

- **Horizonte divido:** El mecanismo de horizonte dividido previene a los routers de ser transmitidos fuera de la interfaz donde fueron recibidos. El horizonte dividido elimina la cuenta a infinito y enruta a los bucle durante la convergencia en interconexiones de redes de una sola trayectoria y disminuye las oportunidades del problema de la cuenta a infinito en interconexiones de redes de trayectorias múltiples.
- **Horizonte dividido con envenenamiento reverso:** El mecanismo de horizonte dividido con envenenamiento reverso permite que se transmitan rutas de regreso a la interfaz de las cuales se recibieron., pero se anuncian en el conteo de hop con 16, que indica que la red está fuera del alcance (en otras palabras, la ruta ha sido envenenada y es inservible a través de esa interfaz).
- **Actualizaciones desencadenadas:** Las actualizaciones desencadenadas permiten que un router anuncie casi inmediatamente cambios en los valores métricos, en vez de esperar el siguiente anuncio periódico. El detonador es un cambio en la métrica en una entrada en la tabla de enrutamiento. Por ejemplo: las redes que no están disponibles pueden anunciarse con un conteo de hop de 16 a través de la actualización desencadenada. Si todos los routers enviaron inmediatamente las actualizaciones desencadenadas, cada actualización desencadenada podría causar una cascada de tráfico de transmisión a través de la interconexión de redes de IP.

Las ventajas del enrutamiento de vector de distancia son que requiere de poco mantenimiento y es fácil de configurar y hacer popular en entornos de redes pequeñas.

El enrutamiento de estado de enlace (el segundo tipo de protocolo de enrutamiento) se diseñó para dominar las desventajas del enrutamiento de vector de distancia. Los routers que utilizan los protocolos de enrutamiento de estado de enlace aprenden acerca del entorno de la red "conociendo" los routers vecinos. Esto se realiza mediante un paquete de "hola", que dice al router vecino a qué redes puede llegar el primero. Una vez que se completa esta presentación, enviará la nueva información de la red a cada uno de los routers vecinos, utilizando un anuncio de estado de enlace. El Open Shortest Path First (OSPF) es un ejemplo de un protocolo de enrutamiento de estado de enlace. Los routers vecinos copian el contenido del paquete y envían el anuncio de estado de enlace a todas las redes adjuntas, excepto la red donde se recibió el anuncio de estado de enlace. Esto se conoce como inundación.

Un router que utiliza un protocolo de enrutamiento del estado de enlace construye un árbol o mapa, de trayectorias más cortas utilizándose a sí mismo como raíz. Este árbol se basa en todos los anuncios de estado de enlace vistos y contiene la ruta para cada destino en la red. Una vez que se construye este árbol, se envía la información de enrutamiento sólo cuando ocurren cambios en la red, en vez de periódicamente como con los protocolos con base en el vector de distancia.

Hay diversas ventajas para el método de estado de enlace, especialmente cuando se compara con los protocolos de enrutamiento con base en el vector de distancia. Algunas ventajas incluyen las siguientes:

- **Tablas de enrutamiento más pequeñas:** Debido a que el router sólo mantiene una tabla de estados de enlace, en vez de una copia de todas las rutas en la red, puede mantener tablas de enrutamiento mucho más pequeñas.
- **Alta escalabilidad:** Los protocolos de estado de enlace no sufren el problema del hop 16 que los protocolos con base en el vector de distancia si padecen, así que son capaces de escalar redes mucho más grandes.
- **Uso más eficiente de ancho de banda de la red:** Debido a que la información del estado de enlace no se intercambia después de que converge la red, las actualizaciones de enrutamiento no consumen el precioso ancho de banda, a menos que haya un corte que fuerce a la red a converger de nuevo.
- **Convergencia más rápida:** Los protocolos de enrutamiento de estado de enlace convergen más rápido que los protocolos con base en el vector de distancia porque las actualizaciones son enviadas tan pronto como sucede un cambio en la red, en vez de tener que esperar las actualizaciones periódicas de los protocolos con base en el vector de distancia.

Una desventaja de los protocolos de estados de enlace es que son más complejos de comprender y configurar que los protocolos del vector de distancia. También se necesita poder de procesamiento adicional en el router, debido a la necesidad de calcular el árbol de enrutamiento.

El enrutamiento puede ser un componente clave en la seguridad de la red, ya que permite determinar qué parte de una red puede ser accesada por otras partes de la red. Por ejemplo: si se tiene una conexión de socios comerciales con una red de una tercera persona, la red de la tercera persona necesitará tener información de enrutamiento con el fin de accesar a cualquier sistema que haya colocado en su DMZ de extranet. Aunque un firewall es la mejor manera de asegurar esta conexión, se puede agregar una capa adicional de seguridad, restringiendo el enrutamiento disponible a la tercera persona. En otras palabras, si sólo se le dice a la red de la tercera persona las rutas a extranet, no podrá enviar paquetes a ninguna otra parte de la red a donde no debe tener acceso.

Sistemas de Prevención y Detección de Intrusión

Las tecnologías disponibles para asegurar las redes son ***los sistemas de detección de intrusión*** (***IDS***) y ***los sistemas de prevención de intrusión*** (inglés, ***IPS***). Un IDS es una solución diseñada para detectar actividades no autorizadas del usuario, ataques y compromisos de la red. Un sistema de prevención de intrusión (IPS) es similar al IDS, excepto que además de detectar y alertar, un IPS también puede actuar para prevenir que suceda una ruptura.

Hay dos tipos principales de IDS/IPS:

- **Con base en la red:** Un IDS con base en la red (NIDS) monitorea el tráfico de la red, utilizando los sensores que se ubican en los lugares clave dentro de la red, a menudo en la zona desmilitarizada o los bordes de red. Estos sensores capturan tráfico de red y analizan los contenidos de los paquetes individuales en busca de tráfico malicioso. Un NIDS accesa el tráfico de red, conectándose al hub, switch de red configurado para el espejo del puerto o la conexión de red.
- **Con base en el servidor:** Un IDS con base en el servidor (HIDS) generalmente tiene un agente de software que actúa como sensor. Este agente monitorea toda la

actividad del servidor en los cuales se instala, incluyendo el monitoreo del sistema del archivo, logs y núcleo para identificar y reportar comportamientos sospechosos. Un HIDS se utiliza típicamente para proteger el servidor en los cuales se instala.

Hay dos metodologías de ejecución comunes utilizadas cuando se coloca un IDS/IPS para proteger una red a partir de Internet. Cada uno tiene ventajas y desventajas:

- **No filtradas:** La instalación de IDS/IPS no filtrado examina la secuencia de datos de Internet cruda. Esto proporciona la mayor cantidad de visibilidad para detectar ataques, pero también significa que hay un volumen importante más grande de datos para monitorear y una posibilidad más alta de falso positivo. También hay una posibilidad de que durante los períodos de mucho tráfico, IDS/IPS tal vez no podría ser capaz de procesar todos los paquetes, así que se podría perder algunos ataques.
- **Filtrado:** Una solución de IDS/IPS filtrado sólo monitorea que el tráfico que pasa por el cortafuegos de filtrado. La ventaja de este modelo es que disminuye dramáticamente la cantidad de información que se necesita monitorear, de este modo también reduce los cambios de falsos positivos y paquetes perdidos durante los volúmenes grandes de tráfico. Sin embargo, hay una pérdida de visibilidad con este modelo, ya que no se puede ver los ataques en el cortafuegos de filtrado.

Tome nota

Históricamente, los IDS y los IPS se han utilizado para asegurar las conexiones de Internet, porque estas conexiones representan típicamente la amenaza más grande para la red. Sin embargo, con la interconectividad de las redes más allá del Internet y la amenaza de ataques de dentro, tiene sentido hacer uso del IDS o IPS en las ubicaciones estratégicas en la red interna. Se debería considerar especialmente hacerlo si la red interna tiene conexiones a redes de terceras personas, tales como clientes, vendedores o socios comerciales

Qué son los Honeypots

Los honeypots, honey nets y padded cells son tecnologías complementarias para las ejecuciones de IDS/IPS. Un ***honeypot*** es una trampa para los hackers, se diseña para distraerlos de los verdaderos objetivos, detectar nuevas vulnerabilidades y explorar y conocer la identidad de los atacantes. Una ***honey net*** es una colección de honeypots utilizados para presentar a un atacante con un entorno de ataque incluso más realista. Finalmente, una ***padded cell*** es un sistema que espera un IDS para detectar a un atacante y luego transfiere al atacante a un servidor especial, donde él o ella no pueden dañar el entorno de producción. Éstas son tecnologías relacionadas y todas pueden utilizarse para añadir una capa adicional a la infraestructura de seguridad.

Como se mencionó previamente, un honeypot es una herramienta de advertencia temprana y vigilancia valiosa. Sin embargo, "honeypot" es un término genérico utilizado para describir cualquier asunto que podría atraer a un atacante. Por consiguiente, aunque el término generalmente se refiere a un software especial que corre en el servido para detectar y analizar ataques, algunas veces puede referirse a otras cosas, como archivos, registro de fechas o incluso espacio de la dirección IP sin utilizar.

Hay una diversidad de tipos diferentes de honeypots, incluyendo los siguientes:

- **Producción:** Un honeypot de producción es una solución relativamente fácil de utilizar. Se usa para distraer a los atacantes de sistemas de producción potencialmente vulnerables y es relativamente fácil de emplear. Estos típicamente

capturan la información limitada y, por lo general, se pueden encontrar en las redes del corporativo. Este tipo de honeypots se utilizan como el sistema temprano de advertencia que mejora un sistema IDS/IPS.

- **Investigación:** Un honeypot de investigación es más complejo que el anterior y es más difícil de utilizar y mantener. Este tipo de honeypot captura la información, que puede utilizarse para desarrollar firmas de ataque, identificar nuevas técnicas de ataque y vulnerabilidades y desarrollar una mejor comprensión del modo de pensar del atacante. Se utilizan en primera instancia para investigaciones por parte de universidades, organizaciones militares u otras del gobierno.

Cuando se hace uso de un honeypot, se debería asegurar que el servidor asociado no contenga información de producción y no se utilice para propósitos de producción. Esto asegura que los datos de producción estén seguros (y, ya que no hay una razón legítima para el tráfico o actividad en el sistema, se puede asumir con seguridad que cualquier actividad que ocurra en el honeypot es actividad malintencionada).

Sin embargo, debería estar consciente de que los honeypots pueden crear riesgos al entorno. Debido a que esencialmente se está utilizando uno como cebo para un atacante, realmente se está atrayendo a los atacantes al entorno de red. Como resultado, se debe estar absolutamente seguro de que estén aislados del entorno de producción. Si no lo están, un atacante podría no brincar de un honeypot al entorno de producción y poner en peligro los sistemas críticos o la infraestructura. Es como tratar de atraer un oso hacia un campamento adjunto para mantenerlo lejos del suyo (siempre hay una posibilidad de que el oso pueda encontrar de cualquier modo el campamento).

Un área en la cual son utilizados especialmente es en la batalla contra el spam. Un desafío relacionado con esto y su filtrado es que los spammers cambian constantemente las técnicas que utilizan para evitar los filtros. También tienen una variedad de técnicas para cosechar las direcciones de correo de los sitios web para la inclusión en las listas de objetivo de spam. Como resultado, las personas que desarrollan filtros invierten mucho tiempo de trabajo para identificar estas técnicas y desarrollar nuevos filtros para combatirlos. Los honeypots son un componente esencial de esta lucha y hay dos tipos que se pueden utilizar para combatir el spam:

- **Honeypot de dirección de email:** Cualquier dirección de email que se dedique a recibir spam para analizarlo puede considerarse honeypot de spam. Un ejemplo de esta técnica es el Proyecto Honeypot, un proyecto de fuente abierta distribuida que utiliza las páginas Honeypot instaladas en sitios web alrededor del mundo junto con direcciones de email etiquetadas únicamente para analizar no sólo la entrega de spam, sino también las técnicas de cosecha de dirección de email.
- **Honeypot de retransmisión abierta de email:** Los re-transmisores abiertos de email son servidores cuyo trabajo es retransmitir los mensajes del servidor de un servidor de correo a otro servidor de correo. Si alguna vez ha utilizado POP3 o IMAP para enviar email por medio de ISP personal, ha utilizado un servidor de transmisión de email. En algunos casos, estos servidores se establecen, así que no necesitan credenciales para enviar email, lo cual es un premio importante para los spammers porque les permite retransmitir anónimamente millones de emails de spam. Establecer un honeypot que parezca ser un re-transmisor abierto puede revelar potencialmente la dirección IP del spammer y proporcionar la captura del spam de volumen. Esto permite, para el análisis a profundidad de las técnicas del spammer, URL de respuesta y direcciones de email y otra información valiosa.

Aunque todas éstas son tecnologías extremadamente emocionantes, se utilizan en muy pocos entornos corporativos. En vez de esto, estas tecnologías se utilizan principalmente por instituciones educativas y firmas de investigación de seguridad. Los profesionales de seguridad de la información corporativa están tan ocupados asegurando el entorno

de ataques que no invierten mucho tiempo en la investigación de patrones de ataque. Mientras no sea exitoso ningún ataque, estos profesionales estarán satisfechos. Aún así, en entornos de alta seguridad en los cuales hay una actividad extensa con base en Internet y datos que requieren capas adicionales de seguridad, los honeypots tal vez puedan ser parte de la defensa de seguridad en capas.

Qué son las DMZ

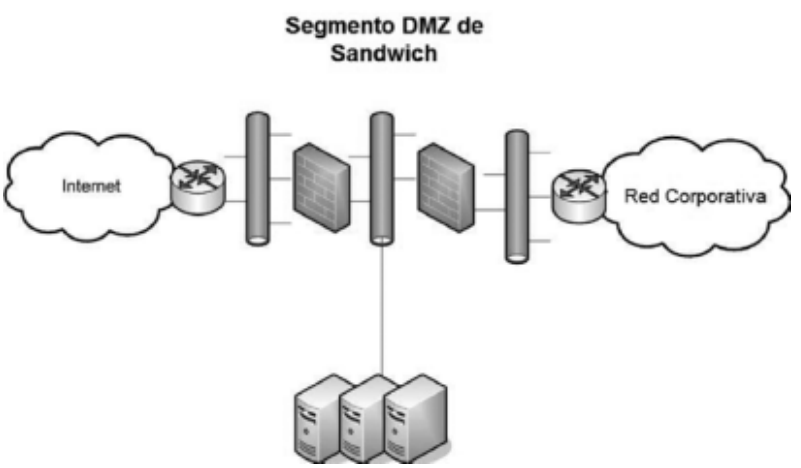
Cuando la mayoría de las personas oye el término ***DMZ*** (acrónimo de ***zona desmilitarizada***), las imágenes de alambre de púas y emplazamientos de armas viene a la mente. Aunque no completamente segura en el alcance de seguridad de información, esta visión no está lejos de la realidad. En la interconexión de computadoras, una DMZ es una configuración de firewall utilizada para asegurar los servidores en un segmento de red. En la mayoría de las DMZ, los servidores en la DMZ se conectan detrás de un firewall que se conecta a la red pública como Internet. Otra configuración común es tener un firewall conectado a una extranet que tiene conexiones con los clientes, proveedores o socios comerciales. DMZ se diseña para proporcionar acceso a los sistemas sin poner en poner en peligro la red interna.

Hay dos configuraciones típicas de DMZ que quizá podría encontrar en los entornos de producción:

- **DMZ de sandwich:** En un modelo DMZ de sandwich (ver Figura 4-3), hay tanto cortafuegos exterior, como interior. El exterior asegura el segmento de red de DMZ de la red (insegura) externa. Los servidores que están hechos para accesar desde la red externa (como Internet) tienen reglas adecuadas configuradas para permitir el acceso seguro. Entonces, el interior se utiliza para agregar una capa adicional de seguridad entre los servidores en la red (de seguridad) interna y la DMZ. El beneficio principal de este modelo es que en caso de que se ponga en peligro el servidor y/o cortafuegos externo en la DMZ, hay una capa adicional de seguridad que protege la red interna. Idealmente, los cortafuegos interiores y exteriores provienen de diferentes proveedores con el fin de asegurar que no se utilice la misma hazaña para poner en peligro ambos. La desventaja mayor de este modelo es que es más compleja de implementar y mantener, es más costosa, debido al cortafuegos extra y, si tiene diferentes proveedores, se necesitará capacitación de personal.

Figura 4-3

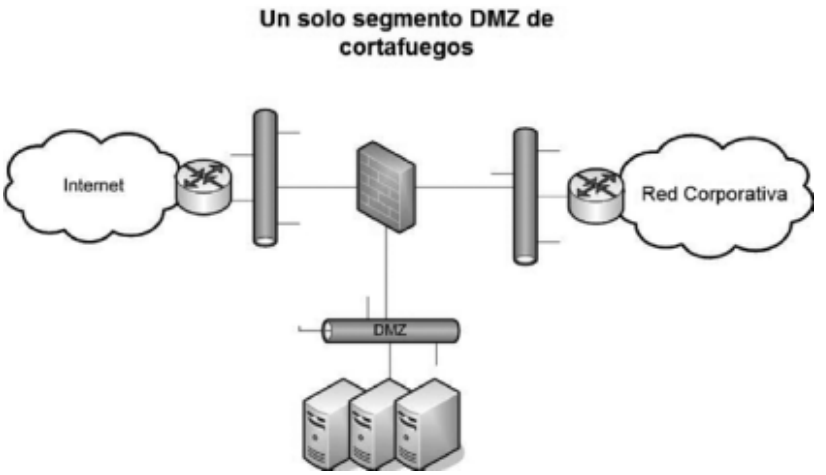
DMZ de sandwich:



DMZ de firewall individual: En una DMZ de firewall individual (ver Figura 4-4), la DMZ es una conexión de red. Esto lleva a una conexión de red externa, una conexión de red interna y una conexión de red de DMZ, todas conectadas al mismo. Aunque esta arquitectura aún permite controlar el acceso a los recursos de DMZ, si se pone en peligro, se podría poner en peligro la red interna. Este modelo es menos costoso que el modelo de sandwich, pero no proporciona un nivel de seguridad tan alto.

Figura 4-4

DMZ de firewall individual



Ahora que se comprende la arquitectura de una DMZ, también debería comprender qué tipos de servidores o servicios podrían utilizarse en una DMZ. Algunos de los más comunes incluyen los siguientes:

- **Servidores web:** Los servidores web son los servidores más comunes hallados en las redes de DMZ. Accesan utilizando HTTP sobre el puerto 80 o HTTPS sobre el puerto 443 para el acceso seguro, los servidores web son comúnmente accesibles a Internet. De hecho, la próxima vez que accese a un servidor web en Internet, se puede contar con el hecho de que está hospedado en una DMZ en alguna parte. Los servidores web agregan una capa adicional de complejidad debido al hecho de que muchas aplicaciones web necesitan comunicarse con una base interna o base de datos para proporcionar algunos servicios especializados. Estas bases de datos a menudo contienen información sensible, así que no se les debe remplazar en la DMZ, ya que no se desea que sean accesadas desde la red insegura (Internet). Un ejemplo de esto podría ser una aplicación de comercio por Internet. Cuando llega a un sitio web del vendedor, los datos del catálogo (incluyendo disponibilidad, precios y descripciones de productos) se halla en la base de datos (algunas veces se referida como base de datos subordinada). Si el servidor de la base de datos también contiene la información crítica como los números de Seguridad Social, información financiera, datos de tarjetas de crédito, tal vez quiera agregar un firewall de aplicación entre el servidor web y el servidor de base de datos. Aunque esto incrementa el costo y complejidad de la solución, se añade una capa extra de seguridad para proteger la base de datos.
- **Servidores de retransmisión de email:** Los servidores de email son otro tipo de servidor a lo que se necesita accesar desde Internet. En los primeros años de interconexión de computadoras, no era común que el email se restringiera de una red de corporativos de la organización. Sin embargo, una vez que las compañías e individuos se conectaban de manera ascendente a Internet, la capacidad de enviar y recibir email de otras compañías de volvió crítico para el éxito de la empresa. Colocando los servidores de retransmisión de email, que se comunican en el puerto 25, en una DMZ, se puede recibir email desde Internet y retransmitirlo de manera

segura a servidores de correo en la red interna. Las capacidades de filtrado de spam se incluyen frecuentemente en estos servidores de retransmisión.

- **Servidores proxy:** Los servidores proxy se utilizan para apoderarse o actuar como intermediario para las solicitudes del usuario de la red interna a Internet y generalmente se utilizan para recuperar información del sitio web. Estos servidores se pueden remplazar en una DMZ para proporcionar seguridad adicional para la navegación de la web. Algunos servidores proxy filtrarán el contenido (incluyendo sitios web inapropiados), añadirán protección de virus y seguridad antispyware e incluso mejorarán el desempeño almacenando en caché las peticiones web.
- **Servidores proxy inversos:** Los servidores proxy inversos se utilizan para proporcionar acceso seguro a las aplicaciones internas desde una red insegura. Aunque estos servidores han sido remplazado en gran parte por las tecnologías VPN, a veces son utilizados para proporcionar el acceso de los empleados a los servidores de email con base en la web en la red interna, proveer acceso a las aplicaciones web internas y, en algunos casos, incluso proporcionar conexiones de servicios de terminales seguras a una red interna.

Traducción de Dirección de Red (NAT)

La Traducción de Dirección de Red (NAT) es una técnica utilizada para modificar la información de dirección de red de un servidor mientras que el tráfico atraviesa un router o cortafuegos. Esta técnica esconde la información de red de una red privada mientras aún permite que se transfiera el tráfico a través de una red pública como Internet.

NAT se creó originalmente como un salto de los problemas de dirección IP. Recuerde que Internet se basa en el juego de protocolo TCP/IP para las comunicaciones entre servidores. Un componente crítico de este juego de protocolo es la dirección IP. En los primeros días de Internet, cuando el protocolo TCP/IP y las direcciones relacionadas estaban desarrollándose, el esquema de dirección de 32 bits (conocido como IPv4) era considerado más adecuado para cualquier crecimiento potencial de la red. Técnicamente, había 4,294,967,296 direcciones únicas disponibles utilizando una dirección de 32 bits e incluso descontando los campos reservados, aún había 3 mil millones de direcciones posibles. En ese tiempo, eso no era suficiente para proporcionar una dirección para cada persona en el planeta, incluyendo niños. Desafortunadamente, los diseñadores de este esquema de dirección desestimaron dramáticamente el crecimiento explosivo de Internet, así como la adopción extendida de TCP/IP en las redes de hogar y negocios (ambas amenazadas para agotar la piscina de direcciones IP de IPv4). Sin direcciones únicas, Internet no podría enrutar exitosamente el tráfico TCP/IP. NAT era la solución resultante para mantener la funcionalidad de Internet, dado el número limitado de direcciones IP disponibles.

Hoy en día, un uso práctico de NAT es que permite utilizar un juego de direcciones IP en una LAN interna y un segundo juego de direcciones IP para la conexión de Internet. Hay un dispositivo (usualmente un router o firewall) ubicado entre las dos redes que proporciona servicios de NAT, gestionando la traducción de direcciones internas a direcciones externas. Esto permite que las compañías utilicen un número grande de direcciones internas que no están registradas, mientras que sólo necesita una fracción del número de direcciones de Internet, por consiguiente, conserva las direcciones. Esto permite reutilizar las direcciones dentro de redes privadas, mientras asegura que las direcciones utilizadas en Internet sigan siendo únicas.

La solución a largo plazo para los problemas de dirección es IPv6 o Protocolo Internet Versión 6, la siguiente generación de protocolos para Internet. Este protocolo se diseña para ofrecer diversas ventajas sobre IPv4, incluyendo el soporte para las direcciones de 128 bits de largo. Esto permite 2^{128} direcciones IPv6 únicas o más de 340 mil millones

de direcciones. Sin embargo, la adopción de IPv6 ha sido lenta, en gran parte debido al uso exitoso de los servidores proxy y NAT para conservar el número de direcciones IPv4 utilizadas actualmente en Internet.

Actualmente, hay dos tipos principales de NAT:

★ Tome nota

Se soporta la Traducción de Dirección de Red (NAT) bajo el Windows Server 2008 por el Servicio de Acceso Remoto y Enrutamiento

- **NAT estática:** La NAT estática traza un mapa de una dirección IP que no está registrada en la red privada a la dirección IP registrada en la red pública, utilizando una base de uno a uno. Este método se utiliza cuando el dispositivo traducido requiere ser accesible desde la red pública. Por ejemplo: el servidor web en su red DMZ podría tener una dirección no registrada de 10.20.30.40 que se traduce por el dispositivo NAT competente a una dirección que da a Internet de 12.4.4.234. De este modo, el usuario que trata de conectarse a ese sitio web puede ingresar 12.4.4.234 y el router o firewall en el otro extremo traducirá esa dirección como 10.20.30.40 cuando el paquete llegue. Esta versión de NAT se utiliza de manera típica junto con las redes extranet o zonas desmilitarizadas.
- **NAT dinámica:** La NAT dinámica traza un mapa de una dirección IP que no está registrada en la red privada a una dirección IP registrada que se selecciona enrutando el dispositivo proporcionando el servicio de NAT desde una piscina de direcciones registradas. Este método se utiliza comúnmente cuando un gran número de sistemas en la red interna necesitan accesar a Internet, pero no tienen el requisito para una dirección estática. Aquí, una dirección de estación de trabajo se traduce a la siguiente dirección registrada disponible en la piscina tan pronto como inicia una conexión a la red pública.

Hay dos implicaciones de seguridad importantes relacionadas con el uso de NAT. Primera, la NAT puede utilizarse para esconder las direcciones de red privadas, lo cual dificulta que un atacante penetre exitosamente en la red privada. Las direcciones que son visibles para un atacante con base en Internet son las direcciones de NAT que se almacenan de modo típico en el firewall, lo cual podría ser uno los dispositivos más seguros de la red.

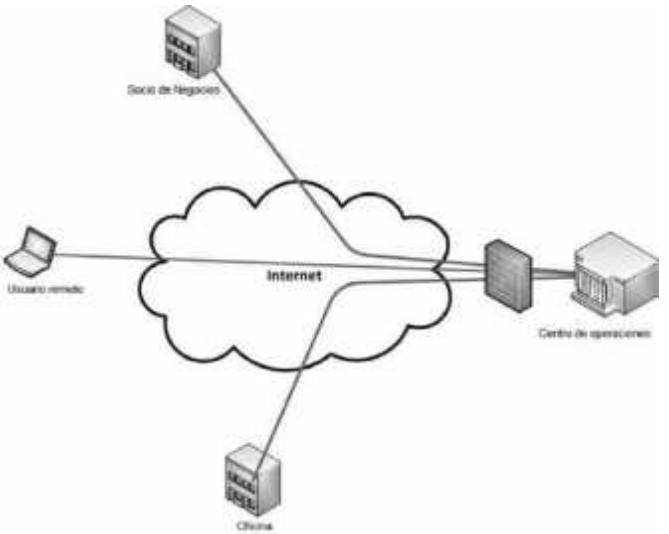
La NAT también presenta un problema único cuando trabaja con el protocolo IPsec (discutido a mayor detalle posteriormente en la lección). Las implementaciones tempranas de IPsec no soportaron la NAT, así que el protocolo IPsec podría no utilizarse cuando se permitió NAT en el entorno. La capacidad de recorrido de NAT se agregó en versiones posteriores del protocolo IPsec, pero IPsec aún requiere que se realicen algunos pasos para funcionara exitosamente con NAT.

▶ *Redes Privadas Virtuales (VPN)*

VPN (Red Privada Virtual) es una tecnología que utiliza túneles codificados para crear conexiones seguras a través de las redes públicas como Internet. Hay una variedad de usos para esta tecnología, pero se muestran tres de las más comunes en la Figura 4-5.

Figura 4-5

Usos de la tecnología VPN



Los empleados a distancia utilizan comúnmente las VPN para accesar a la red interna, para crear conexiones seguras de red en red para conexiones de socios comerciales o sucursales o incluso para crear conexiones seguras de extremo a extremo para aislamiento y seguridad adicional en una red interna. Las VPN utilizan codificación y autentificación para proporcionar confidencialidad, integridad y protección de privacidad de los datos.

Los VPN de acceso a distancia fueron los primeros en introducirse a finales de la década de 1990 y se utilizaron inicialmente junto con módems para proporcionar una conectividad más flexible y segura a las redes de los corporativos. Todo lo que se requería era una conexión de Internet de acceso telefónico y un cliente de VPN y se podría conectar a la red del corporativo sobre una conexión codificada. En resumen, a partir de entonces, con la llegada de las conexiones de Internet de alta velocidad, explotó el uso de tecnologías VPN. Ahora era posible en algunos casos obtener una conexión más rápida en casa vía Internet de alta velocidad que en una sucursal vía conexiones de red típicas. Esta tecnología también permite a los negocios migrar de conexiones de red costosas a conexiones de VPN con base en Internet menos caras.

Las primeras VPN con base en estándares se basaba en el protocolo IPsec. Las VPN con base en IPsec adelantaron rápidamente algunas VPN con base en el propietario que fueron los primeros productos comercializados.

▶ *Internet Protocol Security (IPsec)*

Internet Protocol Security (IPsec) es un conjunto de protocolos con base en estándares diseñados específicamente para asegurar las comunicaciones del Protocolo de Internet (IP). También es un componente de IPv6, la siguiente generación del protocolo IP. IPsec autentifica y codifica cada paquete de IP en una secuencia de datos de IP. Además, IPsec tiene protocolos que pueden utilizarse para establecer la negociación de claves criptográficas y autentificación mutua durante la sesión. IPsec opera en la capa de red del modelo OSI.

IPsec se diseñó para proporcionar seguridad basada en criptografía de alta calidad e interoperable para IPv4 y IPv6. Hoy en día, ofrece un conjunto completo de servicios de seguridad, incluyendo los siguientes:

- Control de acceso
- Revisión de integridad de datos sin conexión

- Autentificación de origen de datos
- Rechazo y detección de repetición
- Confidencialidad utilizando codificación
- Confidencialidad de flujo de tráfico

★ Tome nota

¿Por qué importan las capas? El hecho de que IPsec opera en la capa 3 del modelo OSI significa que se puede utilizar para codificar cualquier tráfico en las capas 4 a través de las 7 del modelo. En términos prácticos, significa que IPsec puede utilizarse para codificar cualquier tráfico de la aplicación

El protocolo IP tiene tres componentes importantes:

- **Cabecera de autentificación: (AH):** AH proporciona protección de integridad para las cabeceras de paquetes, datos y autentificación del usuario. Puede proporcionar opcionalmente protección de transmisión y protección de acceso. AH no puede codificar ninguna porción de paquetes. Para que AH funcione en conjunto con NAT, el protocolo IP número 51 necesita ser permitido a través del firewall.
- **Encapsultating Security Payload (ESP):** ESP proporciona protección de confidencialidad, integridad y autenticidad de los paquetes de dataos. A diferencia de AH, ESP no puede proteger las cabeceras de paquetes (sólo protege los datos). Para que ESP funcione en conjunto con NAT, el protocolo IP número 50 necesita ser permitido a través del firewall.
- **Internet Key Exchange (IKE):** IKE se utiliza para negociar, crear y gestionar las asociaciones de seguridad (SA), lo cual significa que es el protocolo que establece el canal de comunicación de seguridad a los servidores de la red. Para que IKE funcione en conjunto con NAT, el puerto 500 de User Datagram Protocol (UDP) necesita ser permitido a través del firewall.

IPsec puede utilizarse en dos modos diferentes:

- **Modo de transporte (Host–a-Host):** En modo de transporte, sólo se puede encapsular los paquetes de carga útil. Debido a que la cabecera del paquete queda intacta, la información de enrutado original se utiliza para transmitir los datos desde el emisor hasta el receptor. Cuando se utiliza junto con AH, este modo puede no utilizarse en un entorno NAT, ya que la codificación de la cabecera no es compatible con la dirección traducida.
- **Modo túnel (gateway-a-gateway o gateway-a-host):** En modo túnel, el paquete de IP se encapsula completamente y se le da una nueva cabecera. Un servidor/gateway específica en la nueva cabecera IP des-encapsula el paquete. Éste es un modo utilizado para asegurar el tráfico para una conexión VPN de acceso a distancia desde un servidor a distancia a un concentrador VPN en la red interna. Éste también es el modo utilizado para asegurar las conexiones IPsec de sitio a sitio.

Otros Protocolos VPN

Aunque IPsec se considera el protocolo predominante asociado con las VPN, hay otros protocolos que también pueden utilizarse para construir VPN o proporcionar conectividad parecida a la de VPN.

→ Utilizar el Protocolo de Capa de Conexión Segura (SSL) y Seguridad de la Capa de Transporte (TLS)

Uno de los protocolos VPN clave utilizado hoy es SSL/TLS, que es la alternativa principal para que IPsec implemente una solución VPN.

El estándar del protocolo SSL fue propuesto originalmente como estándar por Netscape. Aunque este protocolo se utiliza ampliamente para asegurar los sitios web, se ha formalizado desde entonces en el estándar IETF, conocido como Seguridad de la Capa de Transporte (TLS). El protocolo SSL/TLS proporciona un método para asegurar las comunicaciones cliente/servidor a través de una red y previene escuchar secretamente y la alteración con datos en tránsito. SSL/TLS también proporciona autentificación de extremo y confidencialidad de comunicaciones por medio del uso de la codificación.

Si alguna vez se ha conectado con un sitio web utilizando HTTPS, la versión segura de navegación web HTTP, se ha utilizado el protocolo SSL. Este protocolo proporciona codificación de 128 bits y actualmente es el mecanismo de seguridad destacada para la protección de tráfico web en el banco, comercio en línea, email y esencialmente cualquier sitio seguro que podría encontrarse. En el uso de navegador/usuario final, la autentificación SSL/TLS es en un sentido. Aquí, sólo el servidor se autentifica cuando el cliente se compara con la información ingresada para accesar un servidor para información en el certificado SSL en el servidor (el cliente sabe la identidad del servidor), pero no viceversa (el cliente sigue no autentificado o anónimo). Sin embargo, SSL/TLS también puede realizar la autentificación bidireccional, utilizando certificados con base en el cliente. Esto es particularmente útil cuando este protocolo se utiliza para accesar una red protegida, porque agrega una capa adicional de autentificación para el acceso.

Como se discutió en la sección en IPsec, una VPN crea un túnel seguro a través de la red pública como Internet. Aunque las VPN de SSL aún influencian el concepto de hacer un túnel, crean los túneles de manera diferente que IPsec. Una VPN de SSL establece conectividad utilizando el protocolo SSL. IPsec trabaja en la capa 3 del modelo OSI, mientras SSH funciona en las capas 4 y 5. Las VPN de SSL también pueden encapsular información en las capas 6 y 7, lo cual hace muy flexibles las VPN de SSL.

Una característica adicional de una VPN de SSL es que generalmente conecta utilizando un navegador web, en tanto que la VPN de IPsec generalmente necesita que el software del cliente se instale en el sistema a distancia.

Las VPN de SSL se utilizan de modo predominante para conexiones de VPN de acceso a distancia en las cuales un cliente se conecta a las aplicaciones en una red interna, al contrario de las conexiones de sitio a sitio en los cuales los gateway se utilizan para conectar una red privada distinta por medio de Internet.

Algunos beneficios de la VPN de SSL/TLS sobre las VPN de IPsec incluyen los siguientes:

- **Costo más bajo:** Debido a que VPN de SSL generalmente no tiene clientes, no se tiene los costos de presentación, soporte y actualización de software del cliente:

- **Independencia de plataforma:** Debido a que el acceso a una VPN de SSL se otorga por medio del interfaz estándar de SSL, que es un componente de virtualmente cada navegador web, se soporta prácticamente cualquier sistema operativo que corra un navegador.
- **Flexibilidad de cliente acrecentada:** Como regla general, los clientes de IPsec generalmente se instalan sólo en los sistemas del corporativo. En comparación, debido a la flexibilidad adicional, las VPN de SSL puede configurarse para permitir el acceso desde una diversidad de clientes, incluyendo los sistemas de corporativo, sistemas de hogar, sistemas de proveedores o clientes o incluso máquinas de quiosco en bibliotecas o cafés Internet. Este acceso más amplio puede incrementar mucho la satisfacción del empleado.
- **Soporte de NAT:** Históricamente, la Traducción de Dirección de Red (NAT) ha causado problemas con las VPN de IPsec. Virtualmente todos los vendedores de IPsec han creado soluciones alternativas para este asunto. Aun así, con una VPN de SSL, no se debe tener estos problemas porque SSL trabaja en una capa más alta que IPsec.
- **Control de acceso granular:** Dependiendo del entorno, esto podría considerarse ya sea una ventaja o desventaja. Las VPN de SSL requiere una granularidad más grande de acceso que una VPN de IPsec típica. En particular, en lugar de crear un túnel del servidor hasta la red interna, las VPN de SSL necesitan que cada recurso al que se acceda se defina explícitamente. El lado positivo es que a menos que se defina explícitamente una fuente, un usuario de VPN de SSL puede accesar, lo cual ofrece beneficios de seguridad. Sin embargo, en un entorno complejo, podría añadir gastos indirectos significativos al soporte de VPN.
- **Se necesitan pocas reglas de firewall:** Con el fin de accesar a un gateway de IPsec a través del firewall, se necesita abrir varios puertos para soportar los protocolos individuos para autentificación y el túnel. Con una VPN de SSL, sólo se necesita abrir el puerto 44, lo cual generalmente es fácil debido al predominio del protocolo HTTPS.

Secure Shell (SSH)

Secure Shell (SSH) es un protocolo para la entrada segura a distancia y otros servicios seguros de red en una red. SSH puede utilizarse en diversas aplicaciones a través de plataformas, que incluyen UNIZ, Microsoft Windows, Apple Mac y Linux. Algunas de las aplicaciones soportadas con SSH incluyen las siguientes:

- Entradas seguras
- Ejecuciones seguras de comandos a distancia
- Transferencias seguras de archivos
- Espejos, copias y respaldos seguros de archivos
- Creación de conexiones de VPN (cuando se utilizan junto con el cliente y servidor de Open SSH)

El protocolo SSH consta en tres componentes principales:

- **Protocolo de capa de transporte** Proporciona integridad, confidencialidad y autentificación del servidor con secreto perfecto a plazo.
- **Protocolo de autentificación del usuario:** Proporciona autentificación del cliente en el servidor.
- **Protocolo de conexión:** Hace una multi-plexación del túnel codificado en varios canales lógicos.

Ahora que se han revisado algunos protocolos que se utilizan para asegurar el tráfico en la red, y generalmente a través de las redes públicas como Internet, revisemos una técnica para proporcionar seguridad adicional en la red interna.

Aislamiento del Dominio y del Servidor

A los profesionales de la seguridad constantemente se les pide en las empresas permitir mayores accesos a los recursos para facilitar los requisitos del negocio. Aunque el acceso más fácil y amplio a los recursos puede aumentar la producción de una empresa, también representa desafíos importantes de seguridad. El riesgo de un ataque de virus, dispositivos y usuarios deshonestos y accesos sin autorización a información sensible relacionada con dispositivos sin gestionar o sin autorizar son suficientes para mantener despierto por la noche a cualquier profesional de seguridad de la información.

★ Tome nota

Si desea aprovechar el aislamiento en su entorno, asegúrese de tomar el tiempo para planearlo adecuadamente. Puede ser una implementación compleja y se debe comprender las necesidades antes de comenzar a permitir los protocolos

Un ejemplo podría ser la estación de trabajo de un desarrollador. Muchos desarrolladores sienten que tienen privilegios únicos para hacer su trabajo y, como resultado, quizá podrían ejecutar configuraciones personalizadas, sistemas operativos sin soporte y/o aplicaciones de fuente abierta y tal vez no participarían de los parches del corporativo y de los programas de gestión de configuración. Desde que estas computadoras están conectadas a la red de la organización para accesar a los recursos internos y estas estaciones de trabajo quizá podrían representar desafíos adicionales de seguridad, el aislamiento del dominio y del servidor proporcionan opciones de seguridad adicionales.

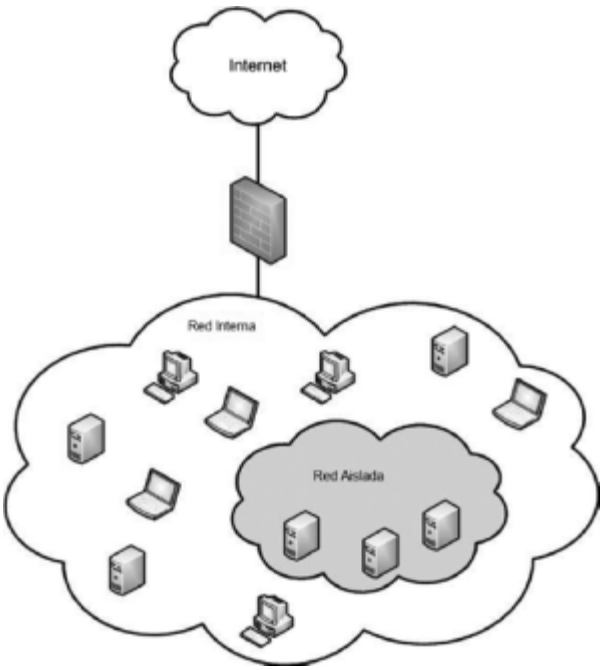
El aislamiento de dominio y del servidor es una solución basada en la IPsec y en Microsoft Directorio activo que permite a los administradores segmentar dinámicamente el entorno de Windows en redes lógicas aisladas más seguras. Estas redes lógicas segmentan con base en la política y se realizan sin necesidad de utilizar los firewalls, implementar VLAN o hacer otros cambios en la red. Los servidores y los dominios pueden asegurarse a través del uso de autentificación y encriptación. Esto crea una capa adicional de protección de política y proporciona otra alternativa para los controles de seguridad discutidos previamente en esta lección.

El aislamiento de dominio y del servidor no debería confundirse con Network Access Protection (NAP). La NAP se enfoca en asegurar que los clientes que están adscritos a la red estén configurados de manera adecuada y autorizada. En comparación, el aislamiento de dominio y del servidor crea zonas de seguridad lógicas dentro de la red y controla quiénes pueden tener acceso a ellas. Ambas son soluciones de seguridad viables, pero tienen objetivos y tecnologías muy diferentes para asegurar el entorno. En una de las configuraciones de alta seguridad, quizá podría utilizar ambas tecnologías para asegurar la protección de la red y sus datos.

La Figura 4-6 proporciona un ejemplo de aislamiento de dominio y del servidor en el cual se puede tener acceso a la red aislada mediante computadoras con la configuración apropiada de Directorio activo y la IPsec.

Figura 4-6

Aislamiento de dominio y del servidor



¿Cómo funciona el proceso de aislamiento? En resumen, la autentificación del entorno aislado se basa en las credenciales de la computadora. Las credenciales pueden ser la expedición de un boleto Kerberos o el Directorio activo puede ser un certificado X.509 distribuido a la computadora mediante una Política de Grupo. Una vez la máquina ha sido autentificada, las políticas de aislamiento relacionadas se hacen cumplir mediante la funcionabilidad de la IPsec dentro de Windows.

Aquí, es importante recordar que la IPsec soporta dos modos. El modo túnel es el modo utilizado con más frecuencia, porque soporta el acceso a distancia utilizado ampliamente y las soluciones de VPN de sitio a sitio que se vuelve ubicuo en el mundo corporativo. El modo de transporte se utiliza para el aislamiento de dominio y del servidor, ya que es un modo que admite con seguridad las comunicaciones de host a host.

▪ Proteger los datos con la seguridad del protocolo

↓ EN RESUMEN

En esta lección, se discutirán diversos protocolos de seguridad, tales como las IPsec, SSL/TLS y SSH. En esta sección, se revisarán varios protocolos adicionales que se utilizan para asegurar los datos. Éstos incluyen un examen de spoofing de protolos, sniffing de red y algunos otros métodos comunes de ataque que podría encontrarse cuando se trabaja para asegurar un entorno de computación corporativo.

☑ Listo para la Certificación

¿Qué protocolo se puede utilizar para proteger datos confidenciales que se envían entre servidores?
—3.4

Uno de los temas más desafiantes para cualquier profesional de seguridad de la información es abordar la idea de la seguridad del protocolo. Ésta ha sido durante mucho tiempo el área de los profesionales de la interconexión, y aunque coinciden en parte obviamente entre la seguridad de información e interconexión, comprenden que la seguridad de protocolo puede ser un verdadero reto para los profesionales de la seguridad de la información, tanto para los principiantes como para los expertos. Con el fin de desarrollar una apreciación de cómo los protocolos de la red pueden impactar exactamente la seguridad, se necesita comenzar la discusión con una revisión del túnel.

▶ *Qué es el Túnel*

Túnel se define como la encapsulación de un protocolo de red dentro de otro. El túnel se utiliza para enrutar un protocolo sin soporte a través de una red o para enrutar con seguridad el tráfico a lo largo de una red insegura. Las VPN emplean una forma de túnel cuando los datos se encapsulan en el protocolo de la IPsec.

✶ Tome nota

¿Qué es PPP? El PPP o Point-to-Point Protocol era un protocolo definido a finales de la década de 1990 que proporcionó un mecanismo de transporte estándar para conexiones de datos point- to-point. Este protocolo principalmente se utilizaba en conjunto con las conexiones de módem y se han retirado paulatinamente, ya que las conexiones de módem han sido remplazadas en gran parte por conexiones de Internet de alta velocidad

Un ejemplo de túnel que se utiliza para mover el tráfico sin soporte a través de la red es el protocolo Generic Routing Encapsulation (GRE). El GRE es un protocolo con base IP utilizado frecuentemente para llevar paquetes de direcciones IP no ruteables a través de una red IP.

Con el fin de comprender por qué se utiliza el protocolo GRE, se necesita discutir la dirección IPv4. Un componente del esquema de dirección de OPv4 es un conjunto de direcciones conocidas con alcances de direcciones reservadas o privadas. Estos alcances incluyen 10.0.0.0 a través de 10.255.255.255, 172.16.0.0 a través de 176.31.255.255 y 192.168.0.0 a través de 192.168.255.255. Estos alcances se asignaron para ayudar a demorar el agotamiento de todas las direcciones de IP de IPv4 y se utiliza típicamente tanto para redes de oficina como de hogares donde no hay un requisito para que se enruten las direcciones a través de una red pública como Internet. Estas redes utilizan generalmente la NAT para permitir el acceso a Internet.

Otra área donde estas direcciones se utilizan es para las redes de desarrollo/laboratorio en un entorno empresarial. Algunas veces hay un requisito para enrutar el tráfico de una red de desarrollo/laboratorio a otra, pero como estas redes utilizan direcciones privadas, podrían no ser enrutables a través de la red de la empresa. Aquí es cuando el GRE se vuelve útil. El tráfico entre los laboratorio puede encapsularse en un túnel GRE, que se puede enrutar sobre la red empresarial sin requerir redirección.

PPTP (Point-to-Point Tunneling Protocol) es un protocolo de VPN patentado desarrollado originalmente por el PPTP Forum, un grupo de vendedores que incluyen Ascend Communications, Microsoft Corporation, 3Com, ECI Telematics y U.S. Robótica. El PPTP se diseñó como una extensión de Point-to-Point Protocol (PPP) para permitir

que PPP se tunelice por medio de una red IP. En un tiempo, PPTP era el protocolo VPM utilizado más ampliamente, pero el estreno de la IPsec tuvo un efecto importante en el uso de PPTP.

Otro protocolo de túnel que alguna vez se utilizó ampliamente es L2TP (Layer 2 Tunneling Protocol), que combinaba las mejores características del protocolo PPTP y L2F (Layer Two Forwarding), que era un protocolo de competencia temprana para PPTP desarrollado por Cisco Systems. Como PPTP, L2TP se diseñaron como una extensión de PPP para permitir que PPP se tunelice por medio de una red IP. El soporte L2TP ser incluyó primeramente en el producto de Microsoft Server con el lanzamiento de Windows Server 2000. Antes de Windows Server 2000, el PPTP era el único protocolo admitido. Diversos vendedores de hardware VPN, incluyendo Cisco, también admitian el protocolo L2TP.

Extensiones de Seguridad del DNS (DNSSEC)

Si alguna vez se ha conectado a un sitio web por nombre, ha utilizado el Sistema de Nombre de Dominio (DNS). El DNS es un servicio utilizado en Internet para resolver direcciones de nombres de dominio completamente calificados (FQDN) a su Protocolo de Internet (IP), utilizando una red distribuida de servidores de nombre. Aquí, se ingresa el nombre del servidor (como www.espn.com) y el DNS asegura que la conexión se dirija a los servidores adecuados. Aunque este servicio es invisible en gran parte para los usuarios finales, el DNS es un elemento crítico de cómo funciona el Internet.

Digamos que se desea revisar los resultados de su deporte favorito utilizando el sitio web de ESPN. Antes del DNS, cuando pregunta: "¿Cuál es la dirección del sitio web de ESPN?", la respuesta podría ser 199.181.132.250. Si es como la mayoría de las personas, olvidaría esos números en menos de 30 segundos, así que probablemente nunca encontraría los resultados de los deportes. En comparación, con el DNS, se puede decir simplemente a la computadora que vaya a www.espn.com y la infraestructura del DNS de Internet traducirá este nombre a la dirección correcta. En otras palabras, el DNA es más como un directorio telefónico: Se escribe un nombre y le da el número correcto.

Sin embargo, el DNS se desarrolló durante los primeros años de Internet, cuando la funcionabilidad era la meta, no la seguridad. Como resultado, el DNS se construyó sin seguridad. En años recientes, se ha explotado esta falta de seguridad con los datos del DNS falsificados, que, entre otros aspectos, redirige las conexiones a sitios web malintencionados. Digamos que escribe la dirección de su banco y, en breve, parece que llegó a su destino. Ingresó su número ID y contraseña para accesar la cuenta, pero no puede entrar. Ahora, digamos que un mes después, averigua que su cuenta está vacía. Lo que pasó fue que la conexión inicial era el resultado de una mala entrada del DNS. En lugar de conectar con el sitio web del banco, se conectó con un duplicado ingenioso que capturó la información de ingreso y dejó que personas malas robaran sus ahorros.

Afortunadamente, el ***DNS Security Extensions (DNSSEC)*** añade provisiones de seguridad al DNS, para que las computadoras puedan verificar que han sido redireccionados a los servidores adecuados. Este nuevo estándar se publicó en marzo de 2005 y lentamente se está adoptando en Internet. El DNSSEC proporciona autentificación e integridad, revisando búsquedas del DNS, asegurando que el tráfico de Internet saliente siempre se envíe al servidor correcto. Esto elimina el problema de los datos de DNS falsificado, ya que no hay manera de falsificar la autentificación adecuada. No sólo encara el problema de redirección de sitios web, sino que también disminuye algunos desafíos relacionados con spam y el uso dominios de correo falso.

El DNSSEC proporciona revisión de integridad y autentificación mediante el uso claves públicas de encriptación. La estructura de nombre de dominio proporciona una jerarquía

de claves de autentificación, creando una cadena de confianza desde la raíz de la jerarquía del DNS hasta el dominio que se consulta. El DNSSEC dirige muchos de los asuntos de seguridad más problemáticos relacionados con la infraestructura de núcleo de Internet, pero conlleva un costo significativo. Como con cualquier implementación de clave pública a gran escala, hacer funcionar el DNSSEC en Internet será un proyecto enormente complejo e intenso de recursos. También hay desafíos relacionados con el mantenimiento web de confianza, creado utilizando claves públicas a una escala de ese tamaño.

Protocol Spoofing

Otra área de preocupación con respecto a los protocolos es el concepto de protocol ***spoofing***. La palabra "spoof" se puede utilizar para referirse a un engaño. Por lo tanto, protocol spoofing es el mal uso de un protocolo para perpetrar un engaño en un dispositivo de red o servidor. Algunas formas comunes de protocol spoofing son las siguientes:

- **ARP spoofing:** ARP (Address Resolution Protocol) spoofing (también conocido como ARP Poisoning) es un ataque en el protocolo utilizado para determinar la dirección de hardware del dispositivo (dirección MAC) en la red cuando se tiene su dirección IP. Es crítico para la entrega adecuada de datos de la red una vez que los datos llegaron al segmento adecuado de LAN. Un ataque de ARP spoofing ocurre cuando un atacante modifica los cachés de ARP de la red y sustituye la dirección IP del servidor de la víctima. Esto permite que el atacante reciba cualquier dato deseado por el servidor original.
- ***DNS spoofing:*** DNS spoofing sucede cuando un atacante puede interceptar una petición de DNS y responde la responde antes que el servidor DNS pueda hacerlo. Como resultado, el servidor víctima se dirige al sitio web equivocado, donde pueden realizarse actividades malintencionadas adicionales. Este ataque se utiliza con frecuencia junto con el sniffing de red, que se discute en la siguiente sección.
- **IP address spoofing:** En un ataque de IP address spoofing, el atacante crea paquetes IP con una dirección IP de fuente falsificada, ya sea para ocultar la identidad del servidor del atacante o hacerse pasar por la identidad del servidor de la víctima. Este tipo de ataque era muy popular en los primeros días de firewalls de análisis de paquetes. Aquí, un atacante husmearía una dirección IP interna desde en firewall exterior, el firewall permitiría el acceso del atacante a la red interna.

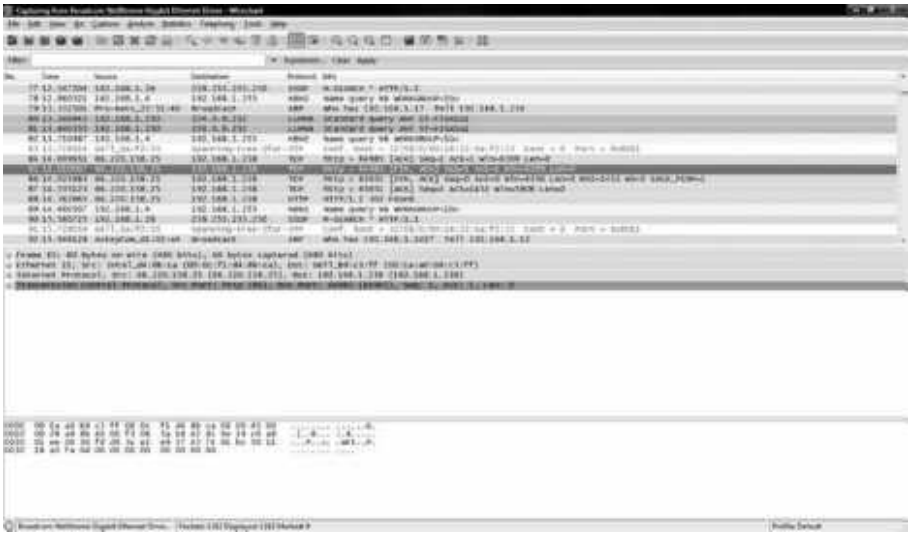
Es importante notar que el término "protocolo spoofing" también tiene otra definición dentro del ámbito de la computación. En particular, el término a veces se utiliza para representar una técnica relacionada con la comprensión de los datos y empleada con el desempeño y rendimiento de la red. Aunque una herramienta valiosa en circunstancias adecuadas, esta forma de spoofing de protocolo no tiene ninguna implicación de seguridad de información.

Sniffing de Red

Sniffing de red es un tipo de análisis que es útil para los administradores responsables de mantener las redes e identificar los problemas de red. Implica conectar un dispositivo a una red con el software adecuado para permitir el acceso a los detalles de los paquetes que atraviesan la red. La Figura 4-7 muestra un ejemplo de Wireshark, una herramienta de sniffing de red de fuente abierta utilizada comúnmente.

Figura 4-7

Wireshark



Como se puede observar en la figura, esta herramienta revela una cantidad importante de información respecto paquetes que se analiza. Para un administrador de red con una comprensión profunda de interconexión, esta información se puede utilizar para identificar problemas de aplicación, latencia de red y variedad de otros errores de red. Desafortunadamente, para un atacante con habilidades similares, la información ofrecida por el sniffing de red proporciona igualmente datos valiosos que se pueden utilizar para propósitos de ataque. Por ejemplo: cualquier dato enviado en texto claro(es decir, sin codificación) generalmente se puede leer directamente desde la red. En los primeros días de Internet, era una cantidad importante de tráfico. En aquella época, leer contraseñas desde paquetes de datos era un ejercicio trivial. Sin embargo, hoy en día, con el uso generalizado de la codificación a través de sitios web seguras y el uso de VPN para acceso remoto, los riesgos representados por el sniffing de red se mitigan ligeramente porque los atacantes ya no pueden leer los contenidos de datos de paquetes. Sin embargo, los atacantes aún pueden obtener información importante respecto a los paquetes de datos que puedan ser útiles en ataques.

Es importante estar conscientes de que el husmeador de la red sólo puede ver el tráfico que cruza el puerto al cual se conecta. Por lo tanto, un husmeador colocado en la LAN en una sucursal no puede capturar el tráfico desde la red de la oficina central. Y, en un entorno de conmutador (switch) que VLAN influencia, se puede limitar la cantidad de tráfico que pasa por cualquier puerto. Los puertos que ofrecen la mayoría de información son puntos de ingreso/egreso de la red, donde se concentra todo el tráfico desde la subred. Esto significa que un atacante no puede capturar directamente el tráfico desde la red, pero no significa que sea seguro. Por ejemplo: un sistema en la red interna que no está infecta con un virus puede terminar corriendo el sniffer de red y proporcionando el tráfico capturado a un servidor a distancia.

Otro desafío de seguridad asociado con los sniffers de red es que hay dispositivos pasivos. A menos que un atacante hay hecho modificaciones a la red para accesar a más información, casi es imposible detectar un sniffer de red. De hecho, podría haber un sniffer de red en un nodo de red más allá de la red interna que podría capturar paquetes respecto al acceso de Internet. En esta circunstancia, incluso no se tiene acceso a la infraestructura de red para buscar cambios.

También se necesita estar consciente de que las redes inalámbricas son particularmente susceptibles a ataques de sniffing de red, debido a la falta de un requisito de puerto. Una vez conectado a una red inalámbrica, un atacante tiene acceso a todo el tráfico en esa red. Por eso es una idea excelente utilizar solamente conexiones codificadas para cualquier cosa que se haga en una red inalámbrica más allá de la navegación general de red.

▶ *Métodos Comunes de Ataque a la red*

★ Tome nota

Un botnet es una red distribuida de computadoras que han sido puestas en riesgo por software malintencionado y está bajo control de un atacante

Se ha cubierto los desafíos de seguridad de información relacionada con la interconexión de computadoras en toda esta lección. La pieza final del rompecabezas de seguridad de red es comprender los tipos de ataques que se espera ver cuando se trabaja para proteger redes de computadoras. Aunque nunca se pueda completar una lista de métodos de ataque, sólo porque los atacantes se presentan constantemente con nuevos tipos de ataque, esta lista cubre las categorías más comunes:

- **Negación de servicio/negación distribuida de ataques de servicio (Dos/DDoS):** El objetivo de una negación de ataque de servicio es inundar la red que se está atacando con cantidades abrumadoras de tráfico, de este modo desconecta infraestructura como un ruteador o firewall. Ya que el atacante no está interesado en recibir respuesta a sus paquetes de ataque, los ataques de DoS son oportunidades ideales para utilizar direcciones spoofed. Las direcciones spoofed son más difíciles de filtrar, porque cada paquete spoofed parece venir de direcciones diferentes, por consiguiente, ocultar la fuente verdadera del ataque. Esto hace retroceder el ataque de manera extremadamente difícil. El nuevo truco para DoS es el DoS distribuido, que influencia los botnets para generar ataques de DoS desde fuentes múltiples. No sólo hace que sea más difícil defenderse del ataque, ya que las computadoras múltiples pueden generar mucho más tráfico que una sola computadora, sino que también dificultan mucho más el rastreo del origen del ataque.
- **IP spoofing para hacer bypass en la seguridad de la red:** Como se discutió previamente, el spoofing de IP es la modificación de paquetes de datos, para que los paquetes de datos de una computadora atacante parece ser una computadora de confianza. Al aparecer como una computadora de confianza, el atacante puede hacer un bypass en las medidas de seguridad de la red, como los filtros de paquete u otras soluciones que se basan en la dirección IP para autentificación. Utilizar este método de ataque en un sistema remoto puede ser extremadamente difícil, porque el atacante puede modificar miles de paquetes con el fin de completar exitosamente el ataque. Este tipo de ataque generalmente funciona mejor cuando hay relaciones confiables entre máquinas. Por ejemplo: no es común en algunos entornos tener servidores UNIX en una red de corporativo donde confíen unos en otros. En esos ejemplos, una vez que el usuario autentifique exitosamente un servidor, él o ella son validados automáticamente en los otros servidores y no necesita una contraseña o ID de usutario para entrar en el sistema. Si un atacante puede hacer spooging exitosamente en una conexión desde una máquina de confianza, él o ella pueden ser capaces de accesar en la máquina objetivo sin una autentificación. Identificar la máquina de confianza se lleva a cabo frecuentemente vía sniffing de red.
- **Ataques Man--in-the-middle:** Un ataque Man-in-the-middle es un tipo de ataque en el cual el atacante se mete en la comunicación entre los extremos de una conexión de red. Una vez que el atacante ha entrado en la secuencia de comunicación, él o ella pueden interceptar los datos que se están transfiriendo e incluso inyectar información falsa en la secuencia de datos. Estos tipos de ataques se utilizan frecuentemente para interceptar tanto las conexiones HTTP y HTTPS. Los sistemas que se conectan a una red inalámbrica son especialmente susceptibles a esta forma de ataque.
- **Ataque de puerta trasera:** Los ataques de puerta trasera son ataques contra una pieza funcional que se dejó abierta en el software que permite el acceso al sistema

o la aplicación de software sin el conocimiento del propietario. Muchas veces, los desarrolladores de la aplicación dejaron abiertas estas puertas traseras, pero la prueba de código actual ha disminuido dramáticamente el número de puertas traseras encontradas en un software comercial. Una versión más común de este ataque sucede cuando los administradores del sistema crean cuentas que pueden utilizar en caso de que se les pida dejar una compañía. Por consiguiente, como profesional de seguridad de información, uno de los objetivos debería ser validar todas las cuentas del sistema que pertenecen a los empleados por lo menos una vez al año.

- **Envenenamiento DNS (DNS poisoning):** Un ataque DNS poisoning es un ataque contra la información almacenada en memoria en el servidor de DNS. Cuando se realiza una solicitud de DNS, el resultado de la petición se almacena en el servidor de DNS, de manera que se regrese con más rapidez las solicitudes posteriores para el mismo servidor, sin pedir una búsqueda por parte del servidor de DNS externo. Desafortunadamente, estos archivos almacenados en caché no son particularmente seguros y los atacantes pueden dirigirse a los archivos para insertar una dirección de IP falsos para una entrada de servidor específico en el caché. Cuando esto sucede, cualquier servidor que hace una solicitud para ese sitio desde el servidor de DNS envenenado será direccionado al sitio equivocado. La entrada falsa en el caché continuará hasta que expire el caché y se actualice.
- **Ataque de reinyección (SQL injection attack):** Este ocurre cuando un atacante puede capturar una secuencia de datos intacta desde una red, utilizan un sniffer de red, modificar ciertos componentes de la secuencia de datos y luego retransmite el tráfico de regreso a la red para completar el ataque. Por ejemplo: un atacante quizá podría capturar una sesión en la cual se está haciendo una comprar, modificar la dirección de entrega y retransmitir el tráfico para colocar una orden que sería entregada a su dirección.
- **Claves de codificación débiles:** Un ataque contra claves de codificación débiles es exitoso cuando las claves tienen un valor que permite romper la codificación. Una vez que ocurre, el atacante es capaz de accesar los datos que se supone que están codificados. Probablemente el ejemplo de más alto perfil de ataque fue la debilidad explotada en el estándar de seguridad Wired Equivalent Privacy (WEP) utilizado junto con las redes inalámbricas. Pensada para utilizarse en las redes inalámbricas de seguridad, se descubrió que las claves WEP eran débiles y que se podrían romper si se capturar 5 ó 10MB de tráfico inalámbrico. Este tráfico quizá podría correr a través de una de muchas herramientas publicadas por la comunidad hacker y el resultado sería la clave WEP, que permite que u atacante lea la información protegida con WEP. Éste es otro ejemplo de un ataque exitoso que se basa en un sniffer de red.
- **Ingeniería social:** Los ataques de ingeniería social ocurren cuando un atacante contacta con un empleado de la organización e intenta extraer información útil de esa persona. Esta información quizá pueda utilizarse para ayudar a conseguir un ataque diferente. Con la ingeniería social, un atacante generalmente intenta aparecer tan inofensivo o respetuoso como sea posible. Generalmente, él o ella harán varias preguntas en un intento de identificar vías posibles para explotar durante un ataque. Si un atacante no recibe suficiente información de un empleado, él o ella podrían llegar a otros hasta que tenga suficiente información para la siguiente fase del ataque.
- **Ataque de agujero de seguridad:** Esta categoría de ataque explota un agujero conocido o no en una aplicación o sistema operativo para realizar actividades malintencionadas. Probablemente es una de las vías más comunes de ataque y frecuentemente es utilizada por virus y gusanos. Una práctica de gestión de conexión sólida es la mejor defensa contra este tipo de ataque, especialmente si se asocia con el programa de gestión de agujeros de seguridad.

- **Ataque de desbordamiento de búfer:** Un ataque de desbordamiento de búfer explota pobremente el código escrito, inyectando datos en campos variables e influenciando la respuesta para accesar a información de la aplicación. Este ataque es posible cuando el desarrollador de aplicación no se limita o revisa el tamaño de los datos que se ingresan en el campo de aplicación. Cuando se ingresan datos muy largos para el campo, se crea un error el atacante puede explotar para realizar acciones maliciosas contra la aplicación.
- **Ataque de ejecución de código remoto:** Los ataques de ejecución de código remoto comúnmente corren contra aplicaciones web. Cuando una aplicaicón se codifica de manera inadecuada, un atacante es capaz de correr un código arbitrario a nivel de sistema por medio de la aplicación y utilizar los resultados para accesar los datos o realizar otras acciones no planeadas contra la aplicación o el servidor de aplicación.
- **Ataque de inyección SQL:** Los ataques de inyección SQL son uno de los más antiguos contra las aplicaciones web que utilizan la aplicación de base de datos del servidor SQL. En este tipo de ataque, los caracteres se ingresan en la aplicación web y, dependiendo de la configuración del servidor de la base de datos, los resultados del ataque pueden alcanzar desde la recuperación de información a partir de la base de datos del servidor web hasta permitir la ejecución del código o incluso acceso completo al servidor. Este ataque se basa en las debilidades de la base de datos, así como en las de codificación.
- **Ataque cross-site scripting (ataque XSS):** Los ataques cross-site scripting son, por mucho, los más comunes y potencialmente el método de ataque actual más peligroso contra los usuarios de web. Estos ataques permiten a los hackers hacer bypass en los mecanismos de seguridad proporcionados por el navegador web. Mediante la inyección de scripts malintencionados en las páginas web y la obtención de usuarios para ejecutarlos, un atacante puede conseguir privilegios de acceso elevados para el contenido de páginas sensibles, cookies de sesión y una variedad de información mantenida por el navegador.

Otros métodos de ataque incluyen el password cracking, ataque de diccionarios y los ataques de fuerza bruta, que se cubrieron en la Lección 3.

El componente final de la seguridad de red con el que debe familiarizarse es la seguridad inalámbrica.

▪ Asegurar Redes Inalámbricas

↓ EN RESUMEN

Las LAN inalámbricas se han convertido en una de las formas más populares de acceso de red, rápidamente de extendieron por hogares a negocios y hotspots inalámbricos de acceso público como los que se encuentra en Starbucks o McDonalds. Las redes inalámbricas ofrecen un gran trato de conveniencia, pero ésta debe balancearse con las implicaciones de seguridad de una red que no es contenida en las paredes del edificio. En esta sección, se discute esas implicaciones y se describe algunas de las técnicas que se pueden utilizar para asegurar la red inalámbrica, incluyendo claves codificadas, SSID y filtros de dirección MAC.

☑ Listo para la certificación

¿Qué métodos puede utilizar para asegurar una red inalámbrica? —1.4

Una LAN inalámbrica (WLAN) permite a los usuarios conectarse a una red permaneciendo móviles. Aunque ésta proporciona a los usuarios acceso fácil a la red desde áreas como las salas de conferencia, oficinas, comedores y otras áreas donde las conexiones alámbricas no existen, también proporciona a los atacantes potenciales acceso similar a la red. Muchas redes inalámbricas de corporativos pueden ser accesadas realmente por cualquiera con una laptop y una tarjeta inalámbrica. Si ha utilizado alguna vez una conexión en un vecindario, tal vez ha notado que su computadora detecta redes inalámbricas diferentes de las que está utilizando. Las empresas tienen la misma cuestión que sus vecinos: Están transmitiendo su red a cualquiera dentro del alcance. De hecho, con antenas especializadas, se puede accesar a las redes inalámbricas desde distancias sorprendentemente largas y, si no se tiene cuidado, ese acceso podría ocurrir sin su conocimiento.

En los primeros días de redes inalámbricas, implementar esta tecnología era fácil, pero asegurarla no. Como resultado, hubo batallas entre los usuarios que querían la facilidad de acceso y la movilidad incrementada que la red inalámbrica prometría y personal de seguridad que estuviera consciente plenamente de los riesgos que introducía la interconexión inalámbrica. Como resultado, la mayoría de los corporativos tuvo políticas estrictas que prohibían el uso de redes inalámbricas a redes internas de acceso directo, que requerían frecuentemente que los usuarios emplearan VPN para conectarse desde la red inalámbrica de producción a la red interna. Como consecuencia, algunos usuarios instalarían puntos de acceso inalámbrico bajo sus escritorios y desearían que nadie de seguridad lo notara. Los atacantes manejarían alrededor de estacionamientos buscando estos puntos de acceso inseguro, de manera que rompieran los perímetros de las redes del corporativo y atacarían las redes internas sin protección. Las organizaciones de seguridad de corporativos también realizarían ejercicios similares con esperanza de encontrar conexiones inalámbricas solitarias antes de que lo hicieran lo atacantes. Sin embargo, actualmente, con algunas capacidades nuevas de seguridad disponibles con las redes inalámbricas, ahora es posible ofrecer bien el acceso inalámbrico a las redes internas, disminuyendo tanto la frecuencia de puntos de acceso solitarios, así como el número de recursos requeridos para encontrar y desactivar esos puntos de acceso.

Otra capacidad que se discute cuando se utilizan redes inalámbricas es asegurar que se sintonice adecuadamente la fuerza del radio de punto de acceso. Aunque hay alguna capacidad para sintonizar la señal inalámbrica para disminuir el riesgo de usuarios sin autorización, no es una buena idea confiar en este método, ya que es la primera línea de defensa cuando se intenta mantener segura la red. Con frecuencia, se encontrará que se impacta negativamente el uso mucho más de lo que se mejora la seguridad.

Service Set Identifier (SSID)

El componente más básico de una red inalámbrica es el Service Set Identifier (SSID). Se define un SSID en el estándar IEE 802.11 como un nombre para la WLAN. No proporciona ninguna capacidad de seguridad inherente, aunque especificando el SSID de la WLAN a la que se desea conectar asegurará que se conecta a la WLAN correcta.

Aunque no hay ninguna capacidad de seguridad específica relacionada con un SSID, definitivamente hay algunas consideraciones que deben tomarse en cuenta:

- **Elegir un SSID:** Lo primero que debe hacerse cuando se establece una WLAN es elegir un SSID único. Cada punto de acceso WLAN viene con un aparato de SSID por omisión. Si utiliza el de omisión, hay un riego de que alguno de los vecinos también tenga ése, causando confusión y conflictos. Por consiguiente, asegúrese de seleccionar un SSID único, pero fácil de recordar.
- **Convenciones de nombre:** Ahora que se eligió un SSID, hay algunas medidas que se debe tomar para hacer un poco más desafiante para un atacante identificar al dueño de la WLAN. Generalmente, no es una buena idea para los corporativos transmitir el hecho de que son los dueños de una red inalámbrica particular. Por lo tanto, se debe evitar seleccionar un SSID con base en el nombre de la compañía, líneas de producto de una compañía o cualquier cosa que pudiera permitir que un atacante confirme quién es dueño de la WLAN. En vez, se selecciona un SSID que los empleados puedan recordar, pero que no invite a los ataques. Temas como nombres de ciudades, deportes, personajes mitológicos u otros nombres genéricos de SSID generalmente son elecciones de seguridad.
- **Apagar el SSID:** El SSID se utiliza para identificar la WLAN y permite a las computadoras conectarse a él. Si transmite esta información, entonces los sistemas del cliente pueden buscar redes inalámbricas disponibles y el nombre de la WLNA aparecerá en la lista. Con tan sólo unos clics, se puede conectar a la WLAN. Aunque extremadamente conveniente para los usuarios autorizados, la retransmisión de un SSID hace igualmente fácil para el atacante conectarse del mismo modo. Para prevenir que suceda, se puede apagar la transmisión de SSID para la red, haciéndolo invisible a los navegadores de red inalámbrica ocasional. Sin embargo, el problema con hacer esto es doble. Primero, dificulta a los usuarios autorizados conectarse a la red y, segundo, cualquier atacante que intente entrar por medio de la red inalámbrica probablemente tendría un sniffer inalámbrico, que le mostraría la SSID de la WLAN, ya sea de transmisión o no, ya que esta información está en paquetes inalámbricos. En este caso, generalmente es prudente seleccionar la disminución del uso en vez de ocultar el SSID (es decir, seguridad por medio de oscuridad).

Ahora, veamos algunas técnicas para asegurar una WLAN.

Comprender las Claves

El mejor mecanismo disponible para asegurar una WLAN es utilizar la autentificación y codificación. Las WLAN ofrecen mecanismos de seguridad con base en tres claves para este propósito.

Wired Equivalency Privacy (WEP)

La primera capacidad de seguridad disponible para los usuarios de WLAN fue WEP (Wired Equivalency Privacy). WEP se incluía como parte del estándar IEEE 802.11 original y se pensó para proporcionar la privacidad. Se recomendaba ampliamente en

los primeros días de uso de WLAN, WEP dejó actuar a favor cuando un defecto con el mecanismo de codificación. Este defecto hace relativamente fácil para un atacante crackear la codificación y accesar la red inalámbrica, así que WEP se utiliza generalmente sólo si no hay otra solución disponible o si se utiliza WLAN con dispositivos (como PDA o juegos de mano) o dispositivos más antiguos que requieren WEP.

Uno de los otros desafíos relacionados con WEP era la mezcla confusa de claves utilizada por los vendedores. Algunos vendedores implementaron las claves en HEX, algunos utilizaron caracteres ASCII y algunos emplearon frases de contraseñas. Dependiendo de la versión de WEP, la longitud de claves también podría variar. Esto era particularmente problemático para los usuarios en hogares que querían utilizar equipo a partir de vendedores múltiples. Con frecuencia, los consumidores terminaban con el equipo que no soportaría la WEP de la misma manera.

Acceso Protegido Wi-Fi (WPA) y Acceso Protegido Wi-Fi Versión 2 (WPA2)

El Acceso Protegido Wi-Fi (WPAA) se diseñó como un sucesor interino de WEP. El protocolo WPA implementa la mayoría del estándar IEEE 802.1 li, que se incluyó en el estándar WLAN actualizado. WPA ofrece un nuevo protocolo de seguridad, Temporal Key Integrity Protocol (TKIP), que aunque está relacionado con WEP para asegurar la compatibilidad hacia atrás, añade características nuevas para ayudar la dirección los problemas relacionados con WEP. Desafortunadamente, debido a que THIP utiliza el mismo mecanismo subyacente que WEP, también es vulnerable a una variedad de ataques similares (aunque la posibilidad de ataque es menos importante que WEP).

Acceso Protegido Wi-Fi Versión 2 (WPA2) es la versión con base en estándares de WPA2 implementa todos los estándares IEEE 802.11i.

WPA/WPA2 funciona e dos modos:

- **WPA de clave compartida:** En un WPA de clave compartida, se configura una frase de contraseña y se ingresa tanto en la red del cliente como en la inalámbrica. Es similar a cómo funciona WEP, pero la protección de la frase de contraseña de WPA es mucho más segura debido al uso de codificación fuerte con el cambio automático de claves. Este modo generalmente generalmente es para usuarios en hogares.
- **IEEE 802.1x**: En modo 802.1x, WPA/WPA2 utiliza un servidor de autentificación externo conectado con el estándar EAP (Extensible Authentication Protocol) para permitir la autentificación fuerte para la conexión a WLAN. Un proceso típico de autentificación incluye los siguientes pasos:

  1. **Inicialización:** En la detección de un servidor, el puerto en el swith se permite y establece en estado "sin autorización". Sólo el tráfico 802.1x se permite mientras el puerto está en este estado.

  2. **Iniciación:** El servidor que está intentando conectarse a la WLAN transmite luego los cuadros de EAP-Request Identity para una dirección especial de capa 2 en el segmento de red local. Esto se conoce como autentificador. Luego, el autentificador envía los paquetes al servidor de autentificación RADIUS.

  3. **Negociación:** El servidor de autentificación manda una respuesta al autentificador. Entonces, el autentificador transmite los paquetes al servidor que se conecta. Estos paquetes se utilizan para negociar el método de autentificación EAP.

4. **Autentificación:** Si el servidor de autentificación y el servidor que se conecta acuerdan en el método de autentificación de EAP, entonces se autentifica el servidor que se conecta. Si la autentificación es exitosa, el autentificador establece el puerto en el estado "autorizado" y se permite el tráfico normal. Si no es exitosa, el puerto continúa en estado "sin autorización" y servidor no puede conectarse.

El uso de autentificación 802.1x para asegurar una WLAN generalmente es reservado para grandes entornos corporativos donde hay recursos suficientes para soportar servidores adicionales y soporte requerido por este modo de operación. La autentificación IEEE 802.1x, particularmente cuando se utiliza junto con una solución de autentificación con base en un token, permite una implementación muy segura de WLAN.

Filtros MAC

Como se discutió al principio en esta lección, una dirección MAC la única dirección de hardware de un adaptador de red. Esta información se puede utilizar para controlar qué sistemas pueden conectarse a una WLAN por medio del uso de filtros MAC. Encendiendo el filtrado MAC, se puede limitar el acceso de red sólo para los sistemas ingresando la información de dirección MAC en los filtros MAC. Los puntos de acceso inalámbrico se mantienen en la tabla de direcciones MAC permitidas.

Pros y Contras de tipos de seguridad específicos

Ahora que se ha discutido diferentes mecanismos de seguridad disponibles cuando se trabaja con las WLAN, consideremos algunas de las ventajas y desventajas de cada una:

- **WEP:** WEP es una solución que, aunque mejor que ninguna seguridad, no es particularmente segura. Las vulnerabilidades dentro del esquema de codificación WEP facilita mucho el intento. WEP evitará que los vecinos se conecten a la WLAN del hogar, pero no entorpecerá a un atacante determinado.
- **WPA/WPA2:** WPA/WPA2 es el mejor método de seguridad tanto para seguridad de WLAN de corporativos como de hogares. En el modo clave precompartido, WPA/WPA2 puede asegurar una WLAN con una frase de contraseña que se comparte con los clientes y puntos de acceso inalámbrico. Siempre que se seleccione una frase de contraseña, ésta es una solución muy segura para las redes pequeñas. Las redes de corporativos, donde se puede comprar la infraestructura de autentificación adicional, la seguridad 802.1x disponible dentro de WPA/WPA2 permite una implementación de WLAN más segura. La desventaja de esta propuesta es que es más costosa y significativamente más compleja que otra solución. Este método también requiere soporte significativamente más alto, porque se necesita mantener las cuentas de los usuarios, se debe soportar los servidores adicionales y la ubicación y corrección de fallas es más desafiante. Sin embargo, estos restos pueden estar abrumadas con una arquitectura redundante y bien diseñada para la WLAN.
- **Filtrado de dirección MAC:** El filtrado de dirección MAC es una buena solución para un entorno de oficina pequeña o de hogar, pero tiene desafíos significativos, ya que aumenta el dispositivos permitidos. El mantenimiento manual de una tabla de direcciones MAC se vuelve un reto importante cuando se tiene más de 10 ó 20 dispositivos, especialmente en los entornos donde los sistemas se compran y decomisan regularmente. Cualquier cambio en la lista de dispositivos permitidos requieren actualizar la tabla de filtrado de dirección MAC, que generalmente es un proceso manual. Otro asunto con el filtrado de dirección MAC es que las direcciones MAC pueden sufrir spoofing por parte de alguien con suficiente conocimiento o capacidad para realizar una búsqueda de Internet de una herramienta para cambiar una dirección MAC. Si los hackers pueden obtener la dirección MAC de un sistema

autorizado, pueden resetear la dirección MAD a esa dirección y, de este modo, obtener acceso a la WLAN. Los filtros de dirección MAC son una buena solución para entornos pequeños y estáticos como hogares u oficinas pequeñas. Aunque no detendrán cierto ataque, son un impedimento para asegurar al cual sólo un atacante motivado verdaderamente intentaría hacerle bypass.

La buena noticia cuando se revisa los mecanismos de seguridad disponibles para la red inalámbrica es que hay soluciones disponibles para cualquier situación. En los primeros días de red inalámbrica, las WLAN ofrecían gran conveniencia para los usuarios, pero no seguridad para la protección de una red de compañía. Utilizar el acceso inalámbrico era tan fácil como comprar un punto de acceso inalámbrico y conectarse a la red. Como resultado, se obligó a los departamentos de seguridad a dedicar recursos al rastreo de puntos solitarios de acceso inalámbrico. Afortunadamente, ahora hay herramientas múltiples que se puede utilizar para identificar puntos de acceso solitario. Así que, aunque aún existe el problema, no es tan frecuente como lo era en años pasados.

Resumen de Habilidad

En esta lección se aprendió que:

- Un firewall es un sistema que se diseña para proteger una computadora o red de computadoras de ataques con base en la red. Un firewall hace esto, filtrando los paquetes de datos que atraviesan la red.
- Los firewalls que se basan en el filtrado de paquetes inspeccionan los datos cuando intentan atravesar el firewall. Con base en reglas rudimentarias, estos firewalls permiten todo el tráfico de salida aunque niegan el todo el tráfico que entra o bloquean la entrada de protocolos específicos, como telnet o ftp, a través del ruteador.
- En lugar de analizar cada paquete individual, un firewall a nivel de circuito monitorea las sesiones TCP/IP, monitoreando el protocolo de intercambio entre paquetes para validar una sesión.
- Los firewalls a nivel de aplicación (también conocidos como servidores proxy) trabajan realizando una inspección profunda de datos de aplicación cuando atraviesan el firewall. Se establece las reglas analizando las peticiones del cliente y las respuestas de aplicación y luego se hace respetar la aplicación correcta.
- Los firewalls de niveles múltiples con memoria de estado anterior se diseñaron para proporcionar las mejores características tanto de firewalls a nivel de aplicación como de filtrado de paquetes.
- Network Access Protection (NAP) proporciona al administrador una manera más poderosa para controlar el acceso a los recursos de red. Los controles de NAP se basan en la identidad de la computadora del cliente y si la computadora cumple las políticas de gobierno de la red configurada.
- Las LAN virtuales (VLAN) se desarrollaron como una solución alterna para utilizar ruteadores múltiples. Las VLAN son segmentos lógicos de red utilizados para crear dominios de transmisión separados, mientras se permiten aún los dispositivos en las VLAN para comunicar a la capa 2 sin un ruteador.
- Un sistema de detección de intrusos (IDS) es una solución diseñada para detectar peligros de red, ataques y actividades del usuario sin autorización.
- Un sistema de prevención de intrusos (IPS) es similar a un IDS, excepto que además de la detección y alerta, un IPS también puede tomar acciones para prevenir que ocurra una ruptura.
- Honeypots, honey nets y padded cells son tecnologías complementarias para usos de IDS/IPS. Un honeypot es una trampa para los hackers.

- Una zona desmilitarizada es una configuración de firewall utilizada para asegurar servidores en un segmento de red. En la mayoría de las zonas desmilitarizadas, los servidores en la zona desmilitarizada se conectan detrás de un firewall que se conecta a una red pública como Internet.
- Network Address Translation (NAT) es una técnica utilizada para modificar la información de dirección de red de un servidor mientras el tráfico atraviesa un ruteador o cortafuegos. Esta técnica oculta información de red de una red privada, aunque permite que se transfiera tráfico por medio de una red pública como Internet.
- DNS Security Extensions (DNSSEC) agrega provisiones de seguridad para DNS, de manera que las computadoras puedan verificar que han sido direccionadas a los servidores adecuados.
- El protocol spoofing es el mal uso de un protocolo para perpetrar un engaño en un dispositivo de red o servidor.
- Un ataque de servicio de negación (DoS) desborda la red objetivo con cantidades abrumadoras de tráfico, desconectando la infraestructura como un ruteador o firewall.
- Un ataque man-in-the-middle es un tipo de ataque en el cual el atacante se mete en la comunicación entre los extremos de una conexión de red. Una vez que el atacante ha entrado en la secuencia de comunicación, él o ella pueden interceptar los datos que se están transfiriendo e incluso inyectar información falsa en la secuencia de datos.
- Los ataques de puerta trasera son ataques contra una pieza funcional que se dejó abierta en el software que permite el acceso al sistema o la aplicación de software sin el conocimiento del propietario.
- Un ataque DNS poisoning es un ataque contra la información almacenada en memoria en el servidor de DNS.
- Un ataque de replay ocurre cuando un atacante puede capturar una secuencia de datos intacta desde una red, utilizan un sniffer de red, modificar ciertos componentes de la secuencia de datos y luego retransmite el tráfico de regreso a la red para completar el ataque.
- Un ataque de desbordamiento de búfer explota pobremente el código escrito, inyectando datos en campos variables e influenciando la respuesta para accesar a información de la aplicación.
- Los ataques de inyección SQL son uno de los más antiguos contra las aplicaciones web que utilizan la aplicación de base de datos del Servidor SQL.
- Una LAN inalámbrica (WLAN) permite a los usuarios conectarse a una red permaneciendo móviles.
- Service Set Identifier (SSID) es el nombre de una WLAN. Un servidor que se conecta debe conocer un SSID de WLAN para conectarse.
- Wired Equivalency Privacy (WEP) es el protocolo de codificación de red inalámbrica más antiguo que cayó de gracia cuando se halló un defecto con el mecanismo de codificación.
- El Acceso Protegido Wi-Fi (WPAA) se diseñó como un sucesor interino de WEP.
- Acceso Protegido Wi-Fi Versión 2 (WPA2) es la versión con base en estándares WPA. A diferencia de WPA, WPA2 implementa todos los estándares IEEE 802.11i.
- Una dirección MAC la única dirección de hardware de un adaptador de red.
- Encendiendo el filtrado MAC, se puede limitar el acceso de red sólo para los sistemas ingresando la información de dirección MAC en los filtros MAC.

» Evaluación de Conocimientos

Elección múltiple

Marque con un círculo la(s) letra(s) que correspondan a la(s) mejor(es) respuesta(s).

1. ¿Cuál de los siguientes elementos o problemas se debería considerar cuando se decide utilizar o no un cortafuegos de hardware o software? (Elija todas las opciones que apliquen.)
   a. Sistema operativo del servidor
   b. Conflictos de aplicación
   c. Versión del sistema operativo
   d. Eficiencia de servicio de cortafuegos
   e. Estabilidad
2. ¿Cuáles de las siguientes son capas del modelo OSI? (Elija todas las opciones que apliquen.)
   a. Física
   b. Control
   c. Aplicación
   d. Red
   e. Codificación
3. ¿En qué capa de modelo OSI se hace el ruteado?
   a. Física
   b. Enlace de datos
   c. Transporte
   d. Sesión
   e. Red
4. ¿Cuál es los siguientes es un tipo de firewall válido? (Elija la mejor respuesta.)
   a. Virtual
   b. Red
   c. Filtrado de paquetes
   d. IPsec
   e. Aplicación
5. ¿Cuál de las siguientes piezas de infomación es examinada típicamente por el firewall de inspección con memoria de estado anterior?
   a. Dirección IP del servidor emisor
   b. Dirección IP del servidor receptor
   c. Dirección IP del ruteador
   d. Tipo de paquetes de datos
   e. Tipo de paquetes de datos
6. ¿Cuál es el propósito de NAP? (Elija la mejor respuesta.)
   a. NAP traduce direcciones IP privadas a direcciones IP ruteable en Internet.
   b. NAP permite a un firewall realizar una inspección profunda en los paquetes.

c. NAP proporciona un mecanismo para realizar un análisis de red en los paquetes capturados.

d. NAP controla qué sistemas se permiten para conectarse a la red.

7. ¿Qué tipo de ataque es uno que se basa en que un usuario ejecute un script malintencionado insertado en la página web? (Elija la mejor respuesta.)

   a. Man-in-the-middle
   b. Fuerza bruta
   c. Cross-site scripting
   d. Inyección SQL

8. Acaba de comprar un nuevo punto de acceso inalámbrico para su compañía de servidores de computadoras y quiere asegurar que sólo los sistemas capaces se conecten a la red inalámbrica. Con ese fin, permite el filtrado de dirección MAC y pone las direcciones MAC de todas las computadoras en la tabla. ¿En qué capa de modelo OSI sucede este filtrado?

   a. Física
   b. Enlace de datos
   c. Red
   d. Transporte
   e. Sesión

9. Es el funcionario de Seguridad de Información de una compañía industrial de tamaño mediano y el equipo de ventas utiliza una nueva aplicación de comercio en línea para permitir ventas directas de los productos a los clientes. Para asegurar esta aplicación. hace uso de un firewall de aplicación. ¿En qué capa de modelo OSI sucede este filtrado? (Seleccione todas las respuestas que apliquen.)

   a. Física
   b. Enlace de datos
   c. Red
   d. Presentación
   e. Aplicación

10. ¿Cuáles de los siguientes son componentes de Network Access Protection? (Elija todas las opciones que apliquen.)

    a. Conformidad de dirección MAC
    b. Conformidad de las políticas de salud
    c. Modo de acceso limitado
    d. Modo de dirección IP
    e. Validación de estado de salud

11. ¿Cuál de los siguientes son ataques con base en la contraseña? (Elija todas las opciones que apliquen.)

    a. Ataques de reinyección
    b. Ataquess de sniffer de red
    c. Ataques de fuerza bruta
    d. Ataques Man-in-the-middle
    e. Ataques de diccionarios

12. ¿Qué tipo de ataque se basa en que el atacante engañe el servidor emisor para que piense que su sistema es el servidor receptor y que el servidor receptor piense que es el servidor emisor? (Elija la mejor respuesta.)
    a. Ataque de reinyección
    b. Ataque de fuerza bruta
    c. Ataque Man--in-the-middle
    d. Ataque cross-site scripting (ataque XSS)
    e. Ataque de inyección SQL
13. ¿Cuál de los siguientes sistemas no puede participar en la implementación de NAP? (Elija todas las opciones que apliquen.)
    a. Windows 7 Home
    b. Windows 7 Home Premium
    c. Windows XP Service Pack 2
    d. Windows Vista Ultimate
    e. Windows 7 Professional
14. ¿Cuál de los siguientes es un uso común de una VPN?
    a. Acceso a distancia
    b. Aislamiento del servidor
    c. Detección de intrusos
    d. Conexión extranet
    e. Aislamiento de dominio
15. ¿Cuáles de los siguientes son tipos comunes de protocolos de ruteo? (Elija todas las opciones que apliquen.)
    a. Vector de enlace
    b. Enlace dinámico
    c. Enlace de distancia
    d. Vector de distancia
    e. Estado de enlace

Llene los espacios

1. Es un administrador de red y lo acaban de poner a cargo de registrar el nombre de dominio de la computadora y establecer la DNS, para que la gente pueda accesar a la página de Internet. Aquí, se puede utilizar _____ para asegurar que las entradas de DENS no sean envenenadas por un atacante.
2. Los dos protocolos más comunes que pueden utilizarse para crear una VPN son _____ y _____.
3. Los tres tipos comunes de spoofing de protocolo son _____, _____ y _____.
4. El tipo de ataque que se basa en una debilidad en un sistema operativo o aplicación se conoce como _____.
5. Un ataque que se basa en el acceso al segmento físico de LAN se conoce como ataque _____.
6. Un ataque que registra la ecuencia de datos, los modifica y luego los reenvía se conoce como ataque _____.

7. Los dos tipos comunes de Network Address Translation son _____ y _____.
8. Si se establece una WLAN en un entorno de corporativo y se desea utilizar un servidor RADIUS y 802.1x para asegurar las conexiones, se necesita utilizar claves _____.
9. Los cuatro mecanismos utilizados por NAP para restringir el acceso y hacer cumplir las políticas son _____, _____, _____ y _____.
10. Un(a) _____ se puede utilizar para distraer a un atacante de los sistemas críticos de la red.

» Evaluación de competencias

Escenario 4-1: Utilizando el cortafuegos de Windows

Trabaja para Corporativo ABC. Necesita decirle a los usuarios cómo abrir la consola Firewall de Windows en una computadora que corre Windows 7 y crea una regla de entrada de Firewall de Windows que permite que Internet Explorer se comunique en los puertos 80 y 443. ¿Qué pasos debe seguir este usuario?

Escenario 4-2: Revisando la Tabla de Ruteo

Trabaja para Corporativo Contoso, donde tiene una computadora que corre Windows 7. Ejecute los comandos necesarios para mostrar las rutas actuales. Ahora, añada una ruta a la red 10.24.57.0 utilizando el gateway 192.168.50.1 y mostrar las rutas para confirmar que se haya agregado. Finalmente, elimine la nueva ruta.

» Evaluación de Habilidades

Escenario 4-3: Paquetes de Sniffing

Decidió que quiere desarrollar una mejor comprensión de los paquetes y cómo operan. Por lo tanto, eligió utilizar un sniffer de protocolo, proporcionado por Microsoft llamado Network Monitor para analizar estos paquetes. Cuando se revisa los paquetes, se desea identificar las cuatro partes principales que componen la mayoría. ¿Qué pasos debería realizar para hacerlo?

Escenario 4-4: Revisando los Puertos

Está hablando con el Oficial en Jefe de Información de la compañía. Uno de los programas que necesita accesar es un servidor que está en una zona desmilitarizada que utiliza los siguientes protocolos:

Secure Shell (SSH)
Network News Transfer Protocol
Protocolo Simple de Administración de Red (SNMP)
NetBIOS
Network Time Protocol

El Oficial en Jefe de Información quiere saber qué puerto es y qué puertos están implicados con estos protocolos. ¿Qué debería decirle?

Estación de trabajo lista

→ Defensa a Profundidad

Recuerde de la Lección 1 que el concepto de defensa a profundidad implica proporcionar capas múltiples de seguridad para defender los valores. Esto asegura que aunque un atacante viole una de las capas de la defensa, todavía tenga capas adicionales para mantenerlo(a) fuera de las áreas críticas del entorno. Para utilizar el control de acceso, debe establecer seguridad física que prevenga que los individuos tengan acceso directo a los servidores sin pasar por la red. También debería tener cortafuegos y ruteadores que limiten el acceso en ella. Entonces, puede utilizar cortafuegos de servidor, Control de Cuentas de Usuario y otros componentes para protegerlo.

Además de revisar el control de acceso, tenga en mente la necesidad de autentificación, autorización y cuenta. Para proteger los recursos de la red, aún necesita establecer un sistema que permita el acceso con base en la autentificación y autorización. Y para asegurar que esa violación de seguridad no haya ocurrido, también debe establecer medidas de cuentas que necesiten revisarse regularmente.

Lección 5

Cómo proteger al Servidor y al Cliente

Matriz de Habilidades de la Lección

Habilidad Tecnológica	Dominio del Objetivo	Número de Dominio del Objetivo
Cómo proteger su computadora de Malware (software malicioso)	Entender el malware	2.6
Cómo proteger la computadora Cliente	Entender la protección del cliente	4.1
Cómo proteger el Correo Electrónico	Entender la protección del correo electrónico	4.2
Cómo proteger el Servidor	Entender la protección del servidor	4.3
Cómo asegurar Internet Explorer	Entender la seguridad para Internet	1.3

Términos Clave

- Adware
- Puerta trasera (back door)
- Filtro bayesiano
- Zonas de contenido
- Cookie
- Software malicioso (malware)
- Microsoft Baseline Security Analyzer (MBSA)
- Archivos fuera de línea
- Pharming
- Phishing
- Ventana emergente
- Rootkit
- Secure Sockets Layer (SSL)
- Sender Policy Framework (SPF)
- Spam
- Spyware
- Troyano
- Control de Cuenta de Usuario (UAC)
- Virus
- Virus hoax
- Windows Defender
- Cortafuegos de Windows (firewall de Windows)
- Windows Server Update Server (WSUS)
- Windows Update
- Gusano

Digamos que habla con el Director de sistemas (CIO) de su compañía sobre la seguridad de su red. Particularmente, está tratando de explicarle que ha establecido un método multi-nivel en la seguridad. Tiene cortafuegos y otros dispositivos que protegen los límites de la red en su organización. También tiene protección configurada para los servidores y los clientes. De este modo, si un hacker evade el nivel externo de seguridad, él o ella necesitarán pasar por otro nivel para entrar a los recursos de la red y a la información confidencial.

▪ Cómo proteger la computadora cliente

↓ EN RESUMEN

Los usuarios utilizan las computadoras Cliente para conectarse a servidores y aplicaciones de la red. Debido a que estas están conectadas a la red de una organización, por lo tanto deben ser protegidas.

☑ Listo para la Certificación

¿Qué se necesita para asegurar la computadora Cliente? —4.1

Si ha estado trabajando con computadoras por mucho tiempo, sabe que proteger la computadora Cliente puede ser bastante complicado. La mayoría de estas funcionarán con un sistema operativo de Windows e incluso dentro de una sola organización, tendrá un amplio rango de aplicaciones de software y servicios de red. Debido a que es lo que usan los usuarios para conectarse normalmente a la red de una organización, es importante que las computadoras Cliente se mantengan seguras de malware e intrusiones.

▶ *Cómo proteger su computadora de Malware*

El software malicioso, llamado algunas veces malware, es un software que está diseñado para infiltrarse o afectar al sistema de una computadora sin la aceptación informada del propietario. El término "malware" normalmente se asocia con virus, gusanos, troyanos, spyware, rootkits y adware engañoso. Como Administrador de redes o Técnico en informática, necesita saber cómo identificar el malware, cómo eliminarlo y cómo proteger a una computadora de este.

☑ Listo para la Certificación

¿Sabe cómo es explotado el buffer overflow (almacenaje temporal)? —2.6

Tipos de Malware

Debido a que ahora es bastante común que las computadoras se conecten a Internet, existen más oportunidades que nunca de que las de su organización resulten infectadas por malware. De hecho, durante los últimos años, se ha producido una cantidad impresionante de malware. Como profesional en seguridad, es responsable de proteger a las computadoras de su organización de infecciones. Además, si una en su red resulta infectada de algún modo por malware, debe asegurarse de que esta infección no se disemine a otras.

Muchas formas anteriores de malware se escribían como experimentos o bromas. La mayor parte del tiempo, estas pretendían ser inofensivas y simplemente molestas. Sin embargo, con el paso del tiempo, el malware se convirtió cada vez más en una herramienta del vandalismo o para comprometer información privada. Actualmente, el malware incluso puede ser usado para lanzar ataques de negación de servicio (DoS) en contra de otros sistemas, redes o sitios Web, que causan que dichos sistemas tengan problemas de desempeño o que se vuelvan inaccesibles.

Como se mencionó anteriormente, el malware puede ser dividido en diversas categorías, incluyendo las siguientes:

- Virus
- Gusanos
- Troyanos
- Spyware y adware engañoso
- Rootkits
- Puertas traseras (back doors)

Un ***virus*** informático es un programa que puede copiarse a sí mismo e infectar una computadora sin la aprobación o el conocimiento del usuario. Los virus anteriores normalmente eran alguna forma de código ejecutable que se ocultaba en el sector de inicio de un disco o como un archivo ejecutable (por ejemplo, un nombre de archivo con una

extensión .exe o .com). Más adelante, a medida que los lenguajes macro comenzaron a ser usados en aplicaciones de software (como procesadores de palabras y programas de hojas de cálculo), los creadores de virus se aferraron a esta tecnología, integrando macros maliciosos en documentos de diversos tipos. Desafortunadamente, debido a que un código macro es ejecutado automáticamente cuando se abre un documento, estos documentos pueden infectar a otros archivos y causar un amplio rango de problemas en sistemas informáticos afectados. Actualmente, los sitios Web también presentan una amenaza de virus, ya que pueden estar escritos en diversos lenguajes de programación y escritura y pueden incluir programas ejecutables. Por lo tanto, en cualquier momento en que accede a Internet, su sistema está bajo una constante amenaza de infección.

Un ***gusano*** es un programa auto-reproducible que se copia a sí mismo en otras computadoras en una red sin ninguna intervención del usuario. A diferencia de un virus, un gusano no corrompe ni modifica archivos en la computadora Objetivo. En vez de esto, consume su ancho de banda, y los recursos de su procesador y su memoria, reduciendo la velocidad del sistema o causando que este sea inutilizable. Los gusanos normalmente se diseminan por medio de brechas en la seguridad de los sistemas operativos o de implementaciones de software de TCP/IP.

El nombre de los Troyanos deriva de la historia del caballo de Troya en la mitología griega. En resumen, un ***troyano*** es un programa ejecutable que aparece como un programa deseable o útil. Debido a que parece ser deseable o útil, los usuarios son engañados para descargar y ejecutar el programa en sus sistemas. Después de que el programa es cargado, este puede causar que la computadora de un usuario se vuelva inutilizable, o puede evadir la seguridad del sistema, permitiendo que su información privada (incluyendo contraseñas, números de tarjetas de crédito y número de seguro social) sea accesible para una persona externa. En algunos casos, un caballo de Troya incluso puede ejecutar adware.

El ***spyware*** es un tipo de malware que es instalado en una computadora para reunir información personal de un usuario o detalles sobre sus hábitos de exploración, con frecuencia sin conocimiento del usuario. El spyware también puede instalar software adicional, redirigir su explorador de Web a otros sitios, o cambiar su página de inicio. Un ejemplo de spyware es el capturador de teclado (keylogger), que registra cada tecla presionada por un usuario. Cuando se instala en su sistema, cada vez que escriba números de una tarjeta de crédito, los números de su seguro social, o contraseñas, esa información es registrada y enviada eventualmente o leída por alguien sin su conocimiento. (Sin embargo, debe indicarse que no todos los keyloggers son malos, ya que algunas corporaciones los usan para monitorear a sus usuarios corporativos.)

El ***Adware*** es cualquier paquete de software que reproduce, muestra o descarga automáticamente anuncios a una computadora después de que el software es instalado o mientras la aplicación está siendo usada. Aún cuando el adware podría no ser necesariamente malo, este se usa con frecuencia con intenciones hostiles.

Un ***rootkit*** es un software o dispositivo de hardware diseñado para obtener el control a nivel de administrador de un sistema informático sin ser detectado. Los rootkits pueden tener como objetivo el, un hipervisor (hypervisor), el cargador de arranque, el núcleo del sistema operativo, o menos comúnmente, bibliotecas o aplicaciones.

Una ***Puerta trasera (back door)*** es un programa que le da a alguien control remoto no autorizado de un sistema o inicia una tarea no autorizada. Algunas puertas traseras son instaladas por virus u otras formas de malware. Otras puertas traseras pueden ser creadas por programas en aplicaciones comerciales o con una aplicación personalizada hecha por una organización.

Los virus y gusanos con frecuencia explotan lo que se conoce como buffer overflow (búfer). En todos los programas de aplicación, incluyendo al mismo Windows, existen buffers que contienen datos. Estos buffers tienen un tamaño fijo. Si se envían demasiados datos a estos buffers, ocurre un buffer overflow (desbordamiento). Dependiendo de los datos enviados al desbordamiento, un hacker puede ser capaz de usar el desbordamiento para enviar contraseñas a sí mismo o a sí misma, alterar archivos del sistema, instalar back doors, o causar errores en una computadora. Cuando se ponen en circulación parches para reparar un buffer overflow potencial, el parche agrega un código para revisar el tamaño de los datos enviados al buffer para asegurarse de que este no se desborde.

Cómo Identificar Malware

El primer paso para eliminar malware es detectar que lo tiene. Algunas veces, es fácil ver que está infectado con malware. Otras veces, quizá nunca sepa que lo tiene. Algunos síntomas comunes de malware incluyen los siguientes:

- Mal desempeño del sistema
- Niveles inusualmente bajos de memoria disponible
- Mal desempeño mientras se está conectado a Internet
- Índices disminuidos de respuesta
- Tiempos más largos de encendido
- Ocasiones en las que su buscador se cierra inesperadamente o deja de responder
- Cambios en la página predeterminada o páginas predeterminadas de búsqueda de su explorador
- Ventanas emergentes de anuncios inesperadas
- Adición de barras de herramientas inesperadas en su explorador
- Ocasiones en las que programas inesperados se inician automáticamente
- Inestabilidad para iniciar un programa
- Anomalías en los componentes de Windows u otros programas
- Programas o archivos faltantes
- Mensajes o proyecciones inusuales en su monitor
- Sonidos o música inusuales reproducidos en momentos aleatorios
- Creación y/o instalación de programas o archivos desconocidos
- Aparición de complementos desconocidos en el explorador
- Archivos corruptos
- Cambios inesperados en los tamaños de los archivos

Desde luego, para ver estos síntomas, necesita buscarlos activamente. Por ejemplo, cuando su máquina con Windows se vuelva lenta, podría iniciar el Administrador de Tareas para ver la utilización del procesador y de la memoria. Entonces, podrá observar el proceso continuo para ver qué proceso está usando la mayor cantidad de recursos del procesador y la memoria. También podría revisar los procesos y servicios en la memoria (de nuevo, puede usar el Administrador de Tareas). Además, puede usar la Configuración del Sistema. Por supuesto, para poder determinar qué procesos y servicios son falsos, necesita tener un punto de partida sobre qué procesos y servicios se están ejecutando actualmente en su sistema saludable para propósitos de comparación. Finalmente, para detectar malware, deberá usar un programa de antivirus actualizado y un paquete de antispyware actualizado, que juntos pueden escanear su sistema completo y buscar malware en tiempo real a medida que abre archivos y accede a sitios Web.

Con tantas herramientas que los agresores pueden usar ahora para enviar malware, es fácil ver la importancia de proteger su computadora de todos los tipos de amenazas de malware. Desde luego, al protegerse a sí mismo, tendrá que usar un poco de su propio sentido común.

Actualizaciones de Seguridad y Software de Antivirus para los Clientes

Algunos virus, gusanos, rootkits, spyware y adware obtienen acceso a un sistema por medio de la explotación de huecos de seguridad en Windows, Internet Explorer, Microsoft Office o algún otro paquete de software. Por lo tanto, el primer paso que debe dar para protegerse a sí mismo contra malware, es mantener su sistema actualizado con los últimos paquetes de servicio, parches de seguridad y otras reparaciones críticas.

El segundo paso para proteger su computadora de malware es usar un paquete de software de antivirus actualizado. Además, si su software de antivirus no incluye un componente antispyware, tiene que instalar uno. Además, deberá asegurarse de llevar a cabo una exploración de todo el sistema con su software de antivirus por lo menos una vez a la semana.

Windows Defender es un producto de software de Microsoft que está diseñado para prevenir, eliminar y poner en cuarentena spyware en Microsoft Windows. Este programa le ayudará a proteger su computadora en contra de ventanas emergentes, desempeño lento y amenazas de seguridad causadas por spyware u otro software no deseado detectando y eliminando spyware conocido. Windows Defender presenta protección en tiempo real, un sistema de monitoreo que recomienda acciones en contra del spyware en el momento de ser detectado e interrupciones mínimas para ayudarle a mantener su equipo en funcionamiento. Desde luego, como con cualquier paquete de antivirus, debe mantener Windows Defender actualizado.

Descargar

Para Windows XP, Windows Defender puede ser descargado del siguiente sitio Web:
http://www.microsoft.com/windows/products/winfamily/defender/default.mspx

→ Cómo Usar el Sentido Común con el Malware

★ Tome Nota

Aunque esta lista puede ser de conocimiento común para el personal de TI, todos los usuarios deben recibir recordatorios y capacitación de concientización para ayudar a proteger su red

Para evitar malware, también es importante el uso del sentido común. Por lo tanto, siempre debe seguir los siguientes pasos:

1. No instale software desconocido o software de origen no acreditado.
2. No abra archivos adjuntos de correos electrónicos extraños.
3. No dé clic en hipervínculos de personas desconocidas cuando no sepa qué se supone que hagan los vínculos. Esto se aplica no sólo para hipervínculos enviados por correo electrónico, sino también para hipervínculos enviados usando servicios de mensajería instantánea.
4. Si su cliente de correo electrónico soporta activación automática, desactívela. De otro modo, podría activar automáticamente un virus informático sólo con abrir un correo electrónico.
5. No visite sitios Web dudosos, especialmente sitios pornográficos o sitios que le permitan descargar software, música o videos piratas.

6. Si su explorador de Web te alerta de que un sitio en particular es conocido por hospedar malware, ponga atención a esta advertencia.
7. Al navegar por Internet, si encuentra ventanas emergentes del buscador que le digan que necesita descargar el controlador más actual o revisar su sistema en busca de virus, proceda con precaución.
8. No olvide llevar a cabo respaldos con regularidad. De ese modo, si contrae un virus y pierde algún dato, puede restaurar su sistema a partir de su respaldo.

Cómo eliminar Malware

★ Tome Nota

Asegúrese de que su software de antivirus esté actualizado. Si no está actualizado, no podrá detectar virus más nuevos

Cuando comience a ver cualquiera de los síntomas enlistados anteriormente en esta lección, debe moverse rápidamente para detectar y (si es necesario) eliminar cualquier malware presente en su sistema. Nuevamente, el primer paso en la eliminación del malware es ejecutar un paquete de software de antivirus y llevar a cabo una exploración completa. Si aún no tiene un software de antivirus, este es un buen momento para adquirirlo. Si no puede descargar este software con su computadora, intenta descargarlo en otra máquina, después copiarlo en un disco óptico (como un CD o DVD) o una memoria portátil para transferirlo a su sistema. Si el software encuentra malware y lo elimina, deberá reiniciar su computadora y ejecutar el programa una vez más para asegurarte de que su sistema esté limpio. Si el programa sigue encontrando diferente malware después de reiniciar, deberá seguir repitiendo el proceso hasta que su máquina esté limpia.

★ Tome Nota

Si ha adquirido un paquete de software de antivirus y está teniendo problemas al eliminar malware, no tenga miedo de contactar a la compañía del software para obtener ayuda

Microsoft ofrece Microsoft Security Essentials (MSE), un producto gratuito de software de antivirus que brinda protección contra malware incluyendo virus, rootkits, spyware y Troyanos. Para descargar MSE, visite el siguiente sitio Web:

http://www.microsoft.com/security_essentials/

Si su paquete de software de antivirus sigue encontrando el mismo malware una y otra vez, necesita asegurarse de que no está accediendo a un disco u otro dispositivo que siga infectando su sistema. Quizá también necesite reiniciar Windows en modo seguro e intentar otra exploración. Si tiene la opción de hacerlo, también puede intentar iniciar desde un CD o DVD y ejecutar la exploración.

Si su software no puede eliminar un virus en particular, haga un poco de investigación en Internet. Con frecuencia, puede encontrar instrucciones paso a paso para eliminar malware, incluyendo borrar archivos y claves en el registro. Por supuesto, asegúrese de que las instrucciones provengan de una fuente confiable y de que las sigue con precisión.

Recuerde, si su paquete de antivirus no cuenta con un componente de antispyware, deberá instalarlo por separado. También puede usar Windows Defender.

★ Tome Nota

Debido a que algunos malware tienen capacidades de keylogger, quizá desee actualizar su información de inicio de sesión en sus cuentas en línea cuando encuentre y elimine malware

Microsoft también ofrece la Microsoft Windows Malicious Software Removal Tool, que revisa computadoras ejecutando Windows en busca de infecciones por malware específico y predominante. Microsoft pone en circulación una versión actualizada de esta herramienta el segundo martes de cada mes y según se requiera para responder a incidentes de seguridad. La herramienta está disponible en Microsoft Update, Windows Update y en el Centro de Descarga de Microsoft.

Finalmente, no olvide usar las siguientes herramientas al intentar eliminar malware desconocido:

- Use el Administrador de tareas para ver y detener procesos desconocidos y para detener servicios desconocidos o dudosos.

- Use Services MMC para detener servicios desconocidos o dudosos.
- Use la Configuración del Sistema para desactivar servicios y programas de inicio desconocidos o dudosos.
- En Internet Explorer, asegúrese de desactivar cualquier complemento desconocido o dudoso.

Cómo examinar un Virus Hoax

Un ***virus hoax*** es un mensaje que advierte al receptor de una amenaza inexistente de virus informático, usualmente enviado como un correo electrónico en cadena que le dice al receptor que lo reenvíe a todas las personas que él/ella conozca. Esta es una forma de ingeniería social que juega con la ignorancia y el miedo de las personas. Algunas alarmas falsas pueden decirles que borren archivos clave del sistema que hacen que su sistema funcione apropiadamente. Otros pueden aconsejarle descargar software de Internet para protegerle contra el supuesto virus, cuando en realidad, el software descargado es alguna forma de malware. Los especialistas en antivirus están de acuerdo en que los receptores siempre deben eliminar alarmas falsas de virus cuando las reciban, en vez de reenviarlos.

▶ *Cómo utilizar Windows Updates*

Después de instalar Windows, debe revisar si Microsoft ha puesto en circulación alguna ***actualización de Windows***, incluyendo reparaciones, parches, paquetes de servicio y controladores de dispositivos actualizados. Si existen, deberá aplicarlos a su sistema de Windows. Al agregar reparaciones y parches, mantendrá a Windows estable y seguro. Debe sabe que en algunos casos, Microsoft pondrá en circulación diversas reparaciones o parches juntos en forma de un paquete de servicio o paquete acumulativo.

Una manera para mantener Windows actualizado es usar el programa Windows Update. Este programa explora su sistema para determinar qué actualizaciones y reparaciones necesita su sistema. Después, tendrá la oportunidad de seleccionar, descargar e instalar cada actualización. Vea la Figura 5-1.

Figura 5-1

Windows Update

Para corporaciones, también puede usar el ***Windows Server Update Service (WSUS)*** o el System Center Configuration Manager (SCCM) para mantener sus sistemas actualizados. La ventaja de usar uno de estos dos es que le permiten comprobar un parche, programar las actualizaciones y dar prioridad a las actualizaciones de los clientes. Una vez que determine si un parche es seguro, puede activarlo para su implementación.

Microsoft con regularidad pone en circulación actualizaciones de seguridad el segundo martes de cada mes, conocidas comúnmente como Patch Tuesday. La mayoría de las otras actualizaciones son puestas en circulación según es necesario; estas son conocidas como actualizaciones "out of band". Debido a que las computadoras son usadas frecuentemente como sistemas de producción, deberá comprobar cualquier actualización para asegurarse de que estas no le causen problemas. Aunque Microsoft lleva a cabo pruebas intensivas, ocurren problemas ocasionalmente, ya sea como un bug o como un problema de compatibilidad con software externo. Por lo tanto, asegúrese siempre de tener un buen respaldo de su sistema y archivos de datos antes de instalar parches, de modo que cuente con un plan de retirada si es necesario.

Microsoft clasifica las actualizaciones como Importantes, Recomendadas u Opcionales:

- **Actualizaciones importantes**: Estas actualizaciones ofrecen beneficios significativos, como seguridad, privacidad y confiabilidad mejoradas; además deben ser instaladas a medida que estén disponibles y pueden ser instaladas automáticamente con Windows Update.
- **Actualizaciones recomendadas**: Abordan problemas no críticos o ayudan a mejorar su experiencia informática. Aunque estas actualizaciones no abordan problemas fundamentales con su computadora o con el software de Windows, pueden ofrecer mejoras significativas.
- **Actualizaciones opcionales**: Estas incluyen actualizaciones, controladores o nuevo software de Microsoft que mejoran su experiencia informática. Necesita instalarlas manualmente.

Dependiendo del tipo de actualización, Windows Update puede ofrecerle lo siguiente:

- **Actualizaciones de seguridad**: Una actualización de seguridad es una reparación puesta en circulación de manera general para una vulnerabilidad relacionada con la seguridad de un producto en específico. Las vulnerabilidades de seguridad son clasificadas con base en su severidad, que se indica en el boletín de seguridad de Microsoft como crítica, importante, moderada o baja.
- **Actualizaciones críticas**: Una actualización crítica es puesta en circulación de manera general para un problema específico que aborda un bug crítico sin relación con la seguridad.
- **Paquetes de servicio**: Un paquete de servicio es un conjunto comprobado y acumulativo de hotfixes (parches que atienden problemas específicos), actualizaciones de seguridad, actualizaciones críticas y actualizaciones, así como reparaciones adicionales para problemas encontrados internamente desde la última puesta en circulación del producto. Los paquetes de servicio también podrían contener un número limitado de cambios o características de diseño solicitadas por el cliente. Después de que un sistema operativo es puesto en circulación, muchas corporaciones consideran el primer paquete de servicio como el momento en que el sistema operativo ha madurado lo suficiente para ser usado a lo largo de la organización.

No todas las actualizaciones pueden ser recuperadas a través de Windows Update. Algunas veces, Microsoft puede ofrecer la reparación para un problema específico en la forma de un hotfix o parche acumulativo que pueda instalar. Un hotfix es un paquete único y acumulativo que incluye uno o más archivos que son usados para abordar un problema en

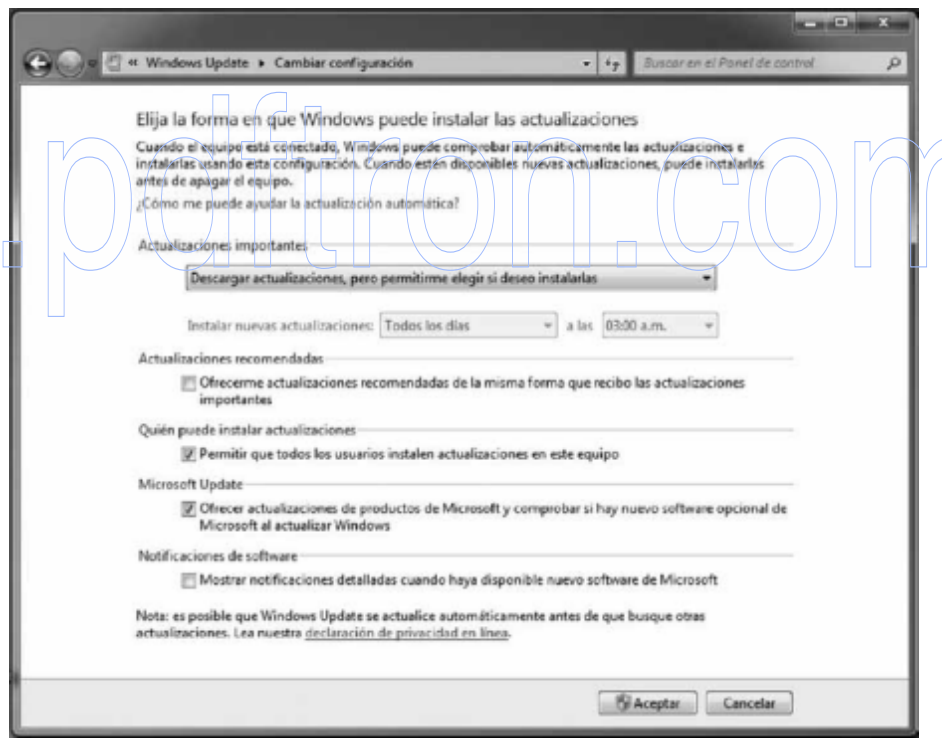
un producto de software, como un bug de software. Comúnmente, los hotfixes son creados para abordar una situación específica de un cliente y con frecuencia no han pasado por pruebas extensivas como los parches recuperados a través de Windows Updates.

Para entornos pequeños, puede configurar su sistema para ejecutar Auto Update (Actualizaciones Automáticas) para asegurarse de que se tengan disponibles actualizaciones críticas, de seguridad y de compatibilidad para ser instaladas automáticamente sin afectar significativamente su uso regular de la Internet. Auto Update trabaja en un segundo plano cuando está conectado a Internet para identificar cuando existen nuevas actualizaciones disponibles y para descargarlas en su computadora. Cuando una descarga es completada, se le notifica y solicita instalar la actualización. En este punto, puede instalar la actualización, obtener más detalles sobre lo que se incluye en la actualización, o permitirle a Windows recordarle sobre la actualización en un momento posterior. Algunas actualizaciones requieren que reinicie su equipo, pero algunas otras no.

Para cambiar sus configuraciones de Windows Update, dé clic en la opción Cambiar Configuraciones en el panel izquierdo de la ventana de Windows Update. Vea la Figura 5-2. Aquí puede especificar qué tipos de actualizaciones desea descargar e instalar automáticamente o puede desactivar Windows Update del todo. También puede especificar si Windows Update buscará actualizaciones para otros productos de Microsoft y/o si instalará cualquier otro software que Microsoft recomiende.

Figura 5-2

Cómo cambiar las configuraciones de Windows Update



Si Windows Update no logra recuperar alguna actualización, deberá revisar sus configuraciones de proxy en Internet Explorer para ver si el programa puede pasar a través de su servidor proxy (si existe alguno) o firewall. También debe revisar si puede acceder a Internet, como por ejemplo entrando a http://www.microsoft.com.

Para ver todas las actualizaciones que han sido instaladas, de clic en Ver Historial de Actualizaciones en la pantalla principal de Windows Update. Si sospecha de un problema con una actualización específica, puede dar clic en Actualizaciones Instaladas en la parte

superior de la pantalla para abrir los programas del Panel de Control. Desde aquí, verá todos los programas y actualizaciones instalados. Si la opción está disponible, puede eliminar la actualización.

Control de Cuenta de Usuario (UAC)

Control de Cuenta de Usuario (UAC) es una característica que comenzó con Windows Vista y está incluido con Windows 7. UAC ayuda a prevenir los cambios no autorizados en su computadora y al hacerlo, le ayuda a proteger su sistema de malware.

Si inicio sesión como administrador, UAC le pide permiso antes de realizar acciones que podrían afectar potencialmente la operación de su computadora o cambiar configuraciones que afecten a otros usuarios. De manera similar, si inicio sesión como usuario estándar, UAC le pedirá una contraseña de administrador antes de realizar dichas acciones. Debido a que UAC está diseñado para prevenir cambios no autorizados (especialmente aquellos creados por software malicioso que quizá no sepa que está ejecutando) necesita leer estas advertencias cuidadosamente y asegurarse de que la acción o programa que está a punto de iniciarse es una que pretendía iniciar.

Como usuario estándar, en Windows 7, puede hacer lo siguiente sin permisos o derechos de administrador:

- Instalar actualizaciones de Windows Update.
- Instalar controladores de Windows Update o controladores que estén incluidos con el sistema operativo.
- Ver configuraciones de Windows.
- Conectar dispositivos de Bluetooth con una computadora.
- Restaurar el adaptador de red y realizar otras tareas de diagnóstico y reparación de la red.

Cuando una aplicación le solicite ascenso o se esté ejecutando como administrador, UAC le pedirá una confirmación, y si se le autoriza, esto le permitirá el acceso como administrador. Vea la Figura 5-3.

Figura 5-3

Confirmación de UAC con Secure Desktop

UAC puede ser activado o desactivado para una cuenta de usuario individual. Desde luego, si desactiva UAC de una cuenta de usuario, su computadora estará en mayor riesgo. Sin embargo, si lleva a cabo muchas tareas administrativas en una computadora, los avisos repetidos de UAC pueden ser molestos y detenerle al hacer ciertas actividades, incluyendo guardar en un directorio de raíz de una unidad si tiene una aplicación que no sea compatible con ella.

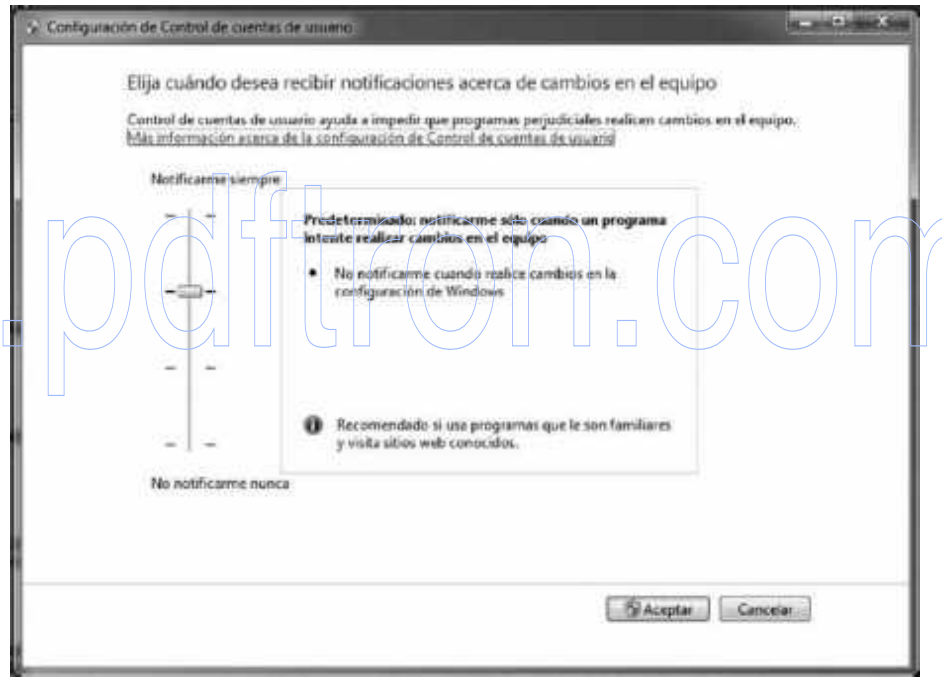
→ Activar o Desactivar UAC

PREPÁRESE. Para activar o desactivar UAC, siga estos pasos:

1. En el **Panel de Control**, dé clic en **Cuentas de Usuario**.
2. En la página de **Cuentas de Usuario**, dé clic en **Cuentas de Usuario**.
3. Haga clic en **Cambiar las configuraciones del Control de Cuentas de Usuario**.
4. Deslize la barra de deslizamiento a las opciones deseadas, como se muestra en la Tabla 5-1. (Vea la Figura 5-4.)

Figura 5-4

Configuraciones de UAC



5. Cuando se le pida reiniciar la computadora, dé clic en **Reiniciar Ahora** o **Reiniciar Más Tarde** según sea apropiado para los cambios que tendrán efecto.

Tabla 5-1

Configuraciones de UAC

Configuración	Descripción	Impacto de Seguridad
Notificarme siempre	Se le notificará antes de que los programas realicen cambios al equipo o a la configuración de Windows que requieran los permisos de un administrador. Cuando se le notifique, el escritorio aparecerá atenuado y deberá aprobar o denegar la solicitud en el cuadro de diálogo de UAC antes de poder cualquier realizar cualquier acción en el equipo. La atenuación del escritorio se denomina escritorio seguro porque no se pueden ejecutar otros programas mientras esté atenuado.	Ésta es la configuración más segura.Cuando se le notifique, debería leer detenidamente el contenido de todos los diálogos antes de permitir que se realicen cambios en el equipo.
Notificarme sólo cuando un programa intente realizar cambios en el equipo	Se le notificará antes de que los programas realicen cambios al equipo que requieran los permisos de un administrador. Se le notificará si trata de realizar cambios en la configuración de Windows que requieran los permisos de un administrador. Se le notificará si un programa que se encuentra fuera trata de realizar cambios en una configuración de Windows.	Por lo general es seguro permitir que se realicen cambios en la configuración Windows sin que se le notifique. Sin embargo, determinados programas incluidos con Windows pueden recibir comandos o datos. El software malintencionado se aprovecha de esta situación y usa estos programas para instalar archivos o cambiar la configuración del equipo. Deberá tener siempre cuidado a la hora de permitir qué programas se pueden ejecutar en el equipo.

Notificarme sólo cuando un programa intente realizar cambios en el equipo (no atenuar el escritorio)	Se le notificará antes de que los programas realicen cambios al equipo que requieran los permisos de un administrador. Se le notificará si trata de realizar cambios en la configuración de Windows que requieran los permisos de un administrador. Se le notificará si un programa que se encuentra fuera trata de realizar cambios en una configuración de Windows.	La configuración es la misma que "Notificarme sólo cuando un programa intente realizar cambios en el equipo" pero no se le notifica en el escritorio seguro.Debido a que el cuadro de diálogo de UAC no se encuentra en el escritorio seguro con esta configuración, es posible que otros programas puedan interferir con el aspecto visual del diálogo. Esto supone un pequeño riesgo para la seguridad si ya tiene un programa malintencionado ejecutándose en el equipo.
No notificarme nunca	No se le notificará antes de realizar cambios en el equipo. Si ha iniciado sesión como administrador, los programas pueden realizar cambios en el equipo sin que sepa nada. Si ha iniciado sesión como usuario estándar, se denegarán los cambios que requieran los permisos de un administrador. Si selecciona esta configuración, tendrá que reiniciar el equipo para completar el proceso de desactivación de UAC. Una vez que UAC está desactivado, los usuarios que inicien sesión como administrador tendrán siempre los permisos de un administrador.	Ésta es la configuración menos segura. Cuando establece UAC para que no notifique nunca, expone el equipo a riesgos potenciales en su seguridad. Si establece UAC para que no notifique nunca, deberá tener cuidado con qué programas ejecuta, porque tendrán el mismo acceso al equipo que el que tiene, incluyendo la lectura y la realización de cambios en áreas del sistema protegidas, los datos personales, archivos guardados y cualquier dato almacenado en el equipo. Los programas también podrán comunicar y transferir información entre cualquier elemento con el que se conecte el equipo, incluido Internet

Usar el Firewall de Windows

Otra herramienta importante para el cliente es un firewall. Como se comentó en la Lección 4, un firewall es un software o hardware que revisa la información proveniente de la Internet o de una red, y puede ser que la bloquee o le permita el paso a través de su computadora dependiendo de sus configuraciones de firewall. Un firewall puede ayudar a prevenir que hackers o software malicioso (como gusanos) obtengan acceso a su computadora a través de una red o la Internet. Un firewall también puede ayudar a evitar que envíe software malicioso a otras computadoras.

Tome Nota

Aún cuando su red pueda contar con un firewall para ayudarle a protegerse del tráfico de Internet no deseado, es una buena idea tener un firewall de servidor para brindarle un nivel adicional de protección. Esto se recomienda especialmente cuando la computadora del cliente es una portátil que puede ser llevada fuera de la red de su organización

Microsoft recomienda que siempre use ***Cortafuegos de Windows (firewall de Windows)***. Sin embargo debido a que algunos paquetes de seguridad y paquetes de antivirus incluyen su propio firewall, se puede elegir ejecutar uno alterno (pero deberá usar únicamente un cortafuegos).

Además del Firewall de Windows encontrado en el Panel de Control, versiones más actuales de Windows incluyen cortafuegos de Windows con Seguridad Avanzada (Advanced Security). Firewall de Windows con Seguridad Avanzada combina un cortafuegos de servidor y seguridad para el Protocolo de Internet (IPSec). Aunque Firewall de Windows con Seguridad Avanzada están unidos estrechamente, este último permite un mayor control. Además, Firewall de Windows con Seguridad Avanzada también brinda seguridad de conexión de una computadora a otra permitiéndole requerir autenticación y protección de datos para comunicaciones por medio de IPsec.

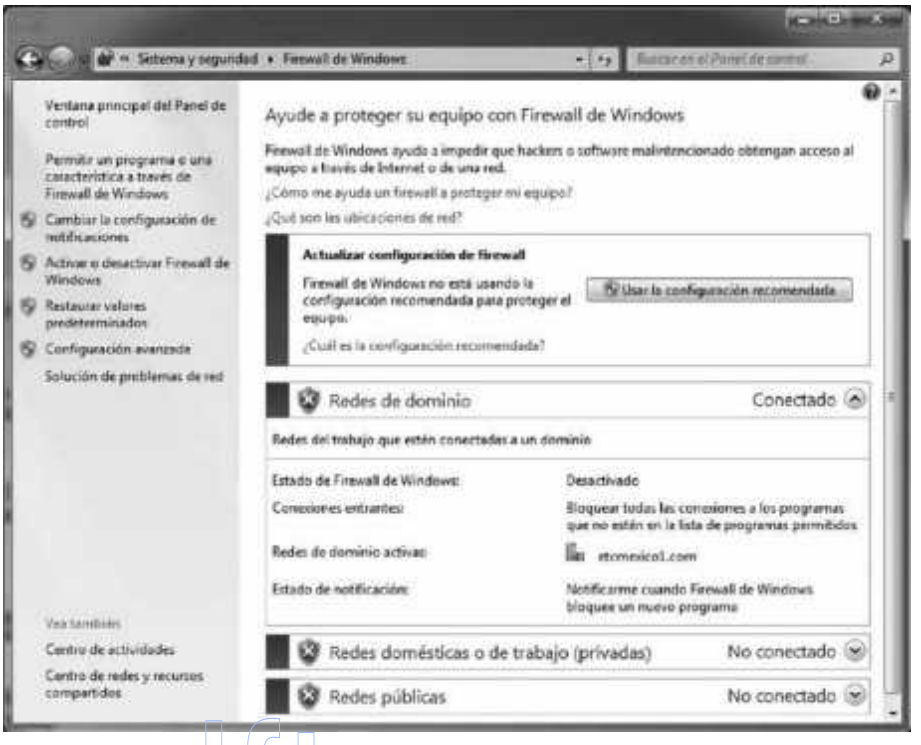
→ Activar o desactivar el cortafuegos de Windows (firewall de Windows)

PREPÁRESE. Para activar o desactivar el cortafuegos de Windows, lleve a cabo los siguientes pasos:

1. Abra el **Panel de Control**.
2. Si está en vista de **Categoría**, dé clic en **Sistema y Seguridad**, y después seleccione **Firewall de Windows**. Si está en vista de **Iconos**, dé doble clic en **Firewall de Windows**.
3. En el cuadro a la izquierda, dé clic en **Activar o Desactivar Firewall de Windows**. Si se le solicita una contraseña o confirmación de administrador, escríbala o acéptela.
4. Dé clic en **Activar Firewall de Windows** debajo de la ubicación apropiada de red para activar Firewall de Windows, o dé clic en **Desactivar Firewall de Windows (no recomendado)** debajo de la ubicación apropiada de red para desactivar Firewall de Windows. Vea la Figura 5-5. Usualmente desea bloquear todo el tráfico de entrada cuando se conecta a una red pública en un hotel o aeropuerto o cuando un gusano informático se está diseminando en la Internet. Cuando bloquea todas las conexiones entrantes, aún podrá ver la mayoría de las páginas Web, enviar y recibir correos electrónicos, y enviar y recibir mensajes instantáneos.

Figura 5-5

Firewall de Windows



5. Si lo desea, seleccione **Bloquear todas las conexiones entrantes, incluyendo aquellas en la lista de programas permitidos** y **Notificarme cuando Firewall de Windows bloquee un nuevo programa**.
6. Haga clic en **OK**.

Por predeterminación, la mayoría de los programas son bloqueados por Firewall de Windows para ayudar a que su computadora sea más segura. Para trabajar apropiadamente, algunos programas podrían requerir que les permita comunicarse a través del cortafuegos.

→ Permitir un programa a través de cortafuegos de Windows (firewalls de Windows)

PREPÁRESE. Para permitir que un programa se comunique a través de Firewall de Windows, lleve a cabo los siguientes pasos:

1. Abra **Firewall de Windows**.
2. En el recuadro a la izquierda, dé clic en **Permitir un programa o característica a través del Firewall de Windows**.
3. Dé clic en **Cambiar configuraciones**. Si se le solicita una contraseña o confirmación de administrador, escriba la contraseña o acepte la confirmación.
4. Seleccione el recuadro de selección junto al programa que desea permitir, seleccione las ubicaciones de red sobre las que desea permitir la comunicación, y dé clic en **OK**.

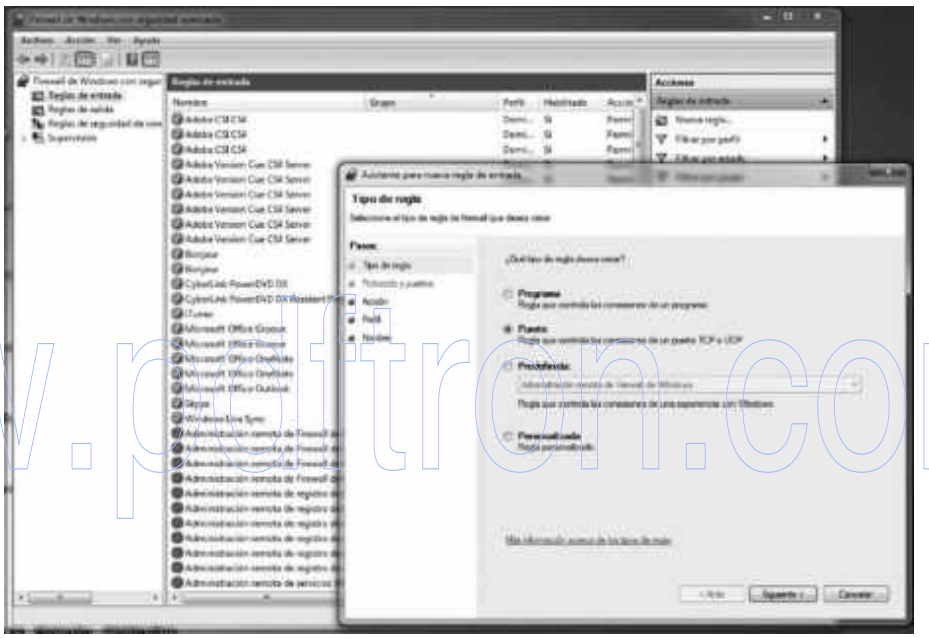
→ Puertos en Firewall de Windows

PREPÁRESE. Si el programa que desea permitir no está en la lista, quizá necesite abrir un puerto. Para abrir un puerto, lleve a cabo los siguientes pasos:

1. Abra **Firewall de Windows**.
2. En el recuadro a la izquierda, dé clic en **Configuracion avanzadas**. Si se le pide una contraseña o confirmación de administrador, escríbala o acéptela.
3. En el recuadro izquierdo del recuadro de diálogo del **Firewall de Windows con Seguridad Avanzada**, dé clic en **Reglas de Entrada**; después, en el recuadro derecho, seleccione **Nueva Regla**.
4. Seleccione **Puerto** y dé clic en el botón **Siguiente**. Vea la Figura 5-6.

Figura 5-6

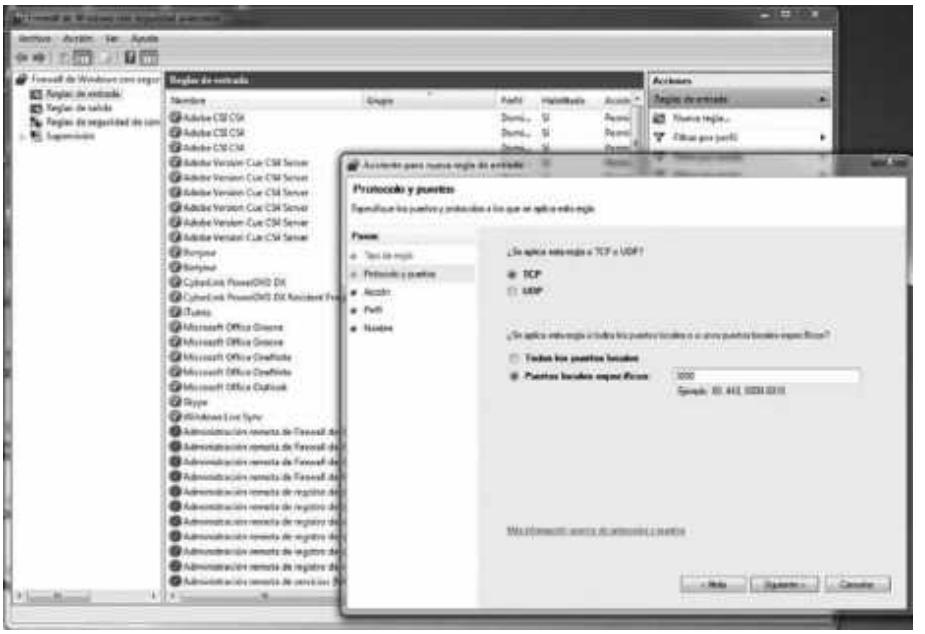
Opciones de Reglas de Entrada



5. Especifique **TCP** o **UDP** y especifique los números del puerto. Dé clic en el botón **Siguiente**. Vea la Figura 5-7.

Figura 5-7

Cómo abrir un puerto



6. Seleccione **Permitir la conexión**, **Permitir la conexión si es segura**, o **Bloquear la conexión**. Dé clic en el botón **Siguiente**.
7. Por predeterminación, la regla se aplicará a todos los dominios. Si no desea que la regla se aplique a un dominio, elimine la selección del dominio. Dé clic en el botón **Siguiente**.
8. Especifique un nombre para la regla y una descripción si lo desea. Dé clic en el botón **Terminar**.

▶ *Usar Archivos Offline*

Los ***Archivos Offline*** son copias de archivos de red que son almacenados en su computadora de modo que pueda acceder a ellos cuando no esté conectado a la red o cuando la carpeta de red que contenga los archivos no esté conectada.

Los archivos offline no están encriptados a menos que elija que lo estén. Quizá desee encriptar sus archivos offline si estos contienen información delicada o confidencial y desee que estos estén más seguros restringiendo el acceso a ellos. La encriptación de sus archivos offline le brinda a un nivel adicional de protección de acceso que trabaja de manera independiente de los permisos del sistema para archivos NTFS (Nuevo Sistema de Archivo Tecnológico). Esto puede ayudar a salvaguardar sus archivos en caso de que su computadora se pierda o sea robada en algún momento.

→ Activar archivos fuera de línea

PREPÁRESE. Para activar los archivos fuera de línea, lleve a cabo estos pasos:

1. Dé clic en el botón de **Inicio** y abra el **Panel de Control**.
2. Busque **Archivos** en el cuadro de texto **Buscar en el Panel de Control** y dé clic en **Administrar archivos fuera de línea**.
3. Dé clic en **Activar archivos fuera de línea**.
4. Si se le pide, reinicie su computadora.

→ Encriptar Archivos Fuera de Línea

PREPÁRESE. Para encriptar sus archivos fuera de línea, lleve a cabo estos pasos:

1. Dé clic en el botón de **Inicio** y abra el **Panel de Control**.
2. Busque **Archivos** en el cuadro de texto **Buscar en el Panel de Control** y dé clic en **Administrar archivos fuera de línea**.
3. Haga clic en la ficha **Encriptación**.
4. 4. Dé clic en **Encriptar** para cifrar sus archivos fuera de línea y después oprima **OK**.

Si elige encriptar sus archivos fuera de línea, encriptará únicamente los archivos almacenados en su computadora, no las versiones de red de los archivos. No es necesario desencriptar un archivo encriptado o carpeta almacenada en su computadora antes de usarlos. Esto se hace automáticamente para sí mismo.

▶ *Bloquear la computadora de un Cliente*

Si trabaja con usuarios finales por un extenso periodo de tiempo, pronto aprenderá que algunos usuarios son sus peores enemigos. Por lo tanto, en algunos casos, deberá considerar bloquear una computadora, de modo que un usuario no pueda dañarla.

A menos que los usuarios individuales tengan la necesidad de ser administradores de sus propias computadoras, ellos deberán ser únicamente usuarios estándar. Esto prevendrá que los usuarios instalen software no autorizado y que realicen cambios en el sistema que podrían hacer que el sistema sea menos seguro. Además, si estos usuarios resultan afectados por malware, el malware únicamente tendrá un acceso mínimo al sistema. Desde luego, se recomendaría usar las opciones de "Ejecutar como" si es necesario, como se comenta en la Lección 2.

Al trabajar dentro de una organización es frecuentemente beneficioso estandarizar cada computadora de la compañía. Por lo tanto, al cambiarse de una computadora a otra, todo será similar. Para mantenerlas estandarizadas, una organización puede elegir usar Políticas Grupales, de modo que los usuarios no puedan acceder a ciertas características (incluyendo el Panel de Control) ni realizar cambios en el sistema que pudiera ser perjudicial.

Permitir a los usuarios instalar software puede:

- Introducir malware a un sistema.
- Evadir las protecciones ya colocadas para protegerse contra virus maliciosos y otras amenazas como los troyanos.

- Causar conflictos con software que ya está en una computadora principal dentro de una organización.

Si no permite a sus usuarios iniciar sesión como administradores, limitará qué software pueden instalar. También puede usar políticas grupales para restringir qué software puede ser ejecutado en la computadora de un cliente.

Windows 7 soporta dos mecanismos para restringir aplicaciones, los cuales están basados en políticas grupales. Estos son:

- Políticas de restricción de software
- AppLockerS

▪ Cómo Proteger Su Correo Electrónico

↓ EN RESUMEN

El correo electrónico se ha convertido en un servicio esencial para prácticamente todas las corporaciones. Desafortunadamente, muchos de los correos electrónicos recibidos por los empleados de una compañía consisten en mensajes no solicitados llamados ***spam*** o correo electrónico basura, algunos de los cuales pueden contener malware y pueden conducir a fraudes o estafas.

☑ Listo para la Certificación

¿Sabe cómo prevenir que se envíen virus a través del correo electrónico?
—4.2

La idea detrás del spam es enviar una gran cantidad de mensajes a granel no solicitados de manera indiscriminada, esperando que unas cuantas personas abran el correo electrónico, naveguen a un sitio Web, compren un producto, o caigan en una estafa. Para las personas que lo crean, el spam tiene costos operativos mínimos. Durante los últimos años, las cantidades de correo electrónico basura se han incrementado exponencialmente, y actualmente, representa al menos 90 por ciento de todos los correos electrónicos en el mundo.

Además del riesgo de malware y fraude asociado al spam, existe también una pérdida de productividad para los receptores de los correos electrónicos a medida que tienen que revisar correos electrónicos no solicitados. Además, el departamento de TI necesitará instalar almacenaje adicional y proveer de suficiente ancho de banda para acomodar el correo electrónico adicional. Por lo tanto, siempre debe de instalar un dispositivo o software de bloqueo de spam que incluya protección antivirus. El programa le brindará un segundo nivel para proteger su red de virus.

▶ *Tratar con el Spam*

Para mantener sus sistemas en ejecución sin problemas, como administrador de redes deberá hacer un esfuerzo por bloquear el spam.

La mejor manera de establecer un sistema de filtrado de spam es en un servidor o dispositivo dedicado o como parte de un dispositivo o servicio de cortafuegos. Puede dirigir todos los correos electrónicos al filtro de spam cambiando su registro de Intercambiador de Correo DNS (MX) para apuntar al servidor o dispositivo antispam. Cualquier correo electrónico que no sea considerado basura será reenviado a sus servidores de correo electrónico internos.

Al establecer un sistema de filtrado de spam, tenga dos cosas en mente. Primero, los sistemas de filtro no atraparan todos los mensajes de spam. Como un paquete de antivirus, una solución de filtrado necesita ser mantenido actualizado y constantemente ajustado. También podría necesitar agregar direcciones de correo electrónico, dominios de correo

electrónico, rangos de direcciones IP, o palabras clave en una lista negra. Cualquier correo electrónico que aparezca en la lista negra será bloqueado automáticamente. Desde luego, necesita tener cuidado al usar una lista negra para asegurarse de que no haga el criterio tan amplio que comience a bloquear correos electrónicos legítimos.

Muchas soluciones antispam también usan una lista negra (blackhole) en tiempo real (RBL), o lista negra en DNS (DNSBL) que puede ser accedida gratuitamente. Las RBLs y DNSBLs son listas de spammers (personas que envían spam) que son actualizadas frecuentemente. La mayoría del software de servidores de correo puede ser configurada para rechazar o marcar mensajes que han sido enviados desde un sitio listado en una o más de dichas listas. Debido a que los spammers buscan maneras para evadir estas listas, esta es sólo una herramienta que puede ayudarle a reducir la cantidad de spam que logra ingresar.

Al identificar un correo electrónico como spam, este usualmente es puesto en cuarentena o almacenado temporalmente en caso de que un correo electrónico haya sido puesto por error en esta categoría. Aunque que el número de mensajes categorizados erróneamente debe de ser relativamente bajo, necesitará capacitar a su personal de servicios de asistencia técnica y posiblemente a sus usuarios para acceder a los correos electrónicos puestos en cuarentena de modo que puedan liberar mensajes colocados erróneamente en su buzón destinado de correo electrónico. Adicionalmente, necesitará agregar la dirección o el dominio de correo electrónico del remitente en una lista blanca de modo que este no sea identificado como spam en el futuro.

Detectar spam puede resultar una labor desalentadora si alguna vez lo ha tenido que hacer de manera manual. Además de las frases obvias de publicidad y otras palabras clave, los sistemas de spam también observarán el encabezado de un correo electrónico para analizar la información sobre el correo electrónico y su origen. Por ejemplo, si tiene su correo en Outlook 2003, abra un mensaje de correo electrónico, abra el menú Ver, y seleccione Opciones. Debajo de Encabezados de Internet, podrá ver el historial para una trayectoria de entrega de correos electrónicos. Para hacer esto en Outlook 2010, primero seleccione el mensaje, después dé clic en el menú Archivo y seleccione Propiedades, debajo de Información.

Para hacer que un mensaje spam se vea como un mensaje legítimo, algunas veces los spammers intentan falsificar una dirección de correo electrónico o dirección IP de donde viene un mensaje. Por ejemplo, si un correo electrónico fue enviado desde un dominio yahoo.com, un sistema antispam podría realizar una búsqueda en reversa usando el registro DNS PTR para ver la dirección IP del dominio yahoo.com. Si esa dirección IP no concuerda con aquella de donde dice el correo electrónico que salió, el mensaje es considerado spam y será bloqueado.

Sender Policy Framework (SPF, Convenio de Remitentes) es un sistema de validación de correos electrónicos diseñado para prevenir spam de correos que usen spoofing (falsificación) de direcciones de origen. SPF permite a los administradores especificar en los registros DNS SPF en el DNS público qué servidores tienen permiso para enviar correos electrónicos desde un dominio en específico. Si no se envían correos electrónicos para un dominio desde un servidor listado en el DNS SPF, se considerará spam y se bloqueará.

Actualmente, los paquetes antispam usan algoritmos especiales, como ***filtros Bayesianos,*** para determinar si un correo electrónico es considerado spam. Estos algoritmos usualmente analizan correos electrónicos recibidos anteriormente y crean una base de datos usando un número de atributos. Después, cuando una computadora recibe un correo electrónico, este comparará ese correo electrónico con los atributos que ha recolectado para determinar si el mensaje es spam.

▶ *Transferencia de Correos Electrónicos*

Protocolo de Transferencia Simple de Correo Electrónico (SMTP,) es uno de los principales protocolos para correo electrónico. SMTP se usa para transferir correos electrónicos de un servidor a otro, y es responsable por el transporte de correo de salida. SMTP usa el puerto TCP 25.

Aunque podría pensar que sus servidores de correo electrónico funcionan nicamente para que los usuarios envíen y reciban correos electrónicos, estos también pueden ser usados para transferir correos electrónicos. Por ejemplo, los servidores Web y de aplicaciones pueden transferir correos electrónicos a través de sus servidores de correo electrónico, como cuando ordena algo por Internet y se le envía un correo electrónico de confirmación.

Normalmente, únicamente desea que sus servidores internos transfieran correos electrónicos a través de sus servidores de correo. Desafortunadamente, los spammers buscan frecuentemente servidores SMTP no protegidos para transferir sus correos electrónicos a través de ellos. Como resultado, no sólo los spammers usan sus servidores SMTP para enviar correos electrónicos, sino que otras organizaciones pueden marcar su servidor o dominio como spammer y podría ser colocado en una de las RBLs o DNSBLs. Para salir de esta lista, necesitará cerrar su hueco de seguridad de modo que otras personas no puedan transferir correos electrónicos a través de su servidor. Después, podrá contactar a las organizaciones que poseen las RBLs o DNSBLs para hacer que lo saquen de su lista.

▪ Cómo Asegurar Internet Explorer

↓ EN RESUMEN

Debido a que la exploración de un sitio Web puede exponerlo a un amplio rango de riesgos, también necesita observar su explorador cuidadosamente para ayudarse a protegerse a sí mismo y a su sistema. Los exploradores actuales incluyen bloqueadores de ventanas emergentes, zonas, y otras características integradas de seguridad.

▶ *Cookies y Configuraciones de Seguridad*

Cuando usa un explorador para acceder a Internet, podría estar revelando información personal y mucho sobre su personalidad. Por lo tanto, necesita tomar medidas para asegurar que esta información no pueda ser leída o usada sin su conocimiento.

☑ Listo para la Certificación

¿De dónde cree que viene la mayor parte del malware?
—1.3

Una ***cookie*** es un pedazo de texto almacenado por el explorador Web de un usuario. Este archivo puede ser usado para un amplio rango de propósitos, incluyendo identificación del usuario, autenticación, y almacenaje de las preferencias de un sitio y contenidos de un carrito de compras. Aunque las cookies pueden darle a un sitio Web gran capacidad, estas también pueden ser usadas por programas de spyware y sitios Web para rastrear a las personas. Desafortunadamente, algunos sitios Web no operarán sin cookies.

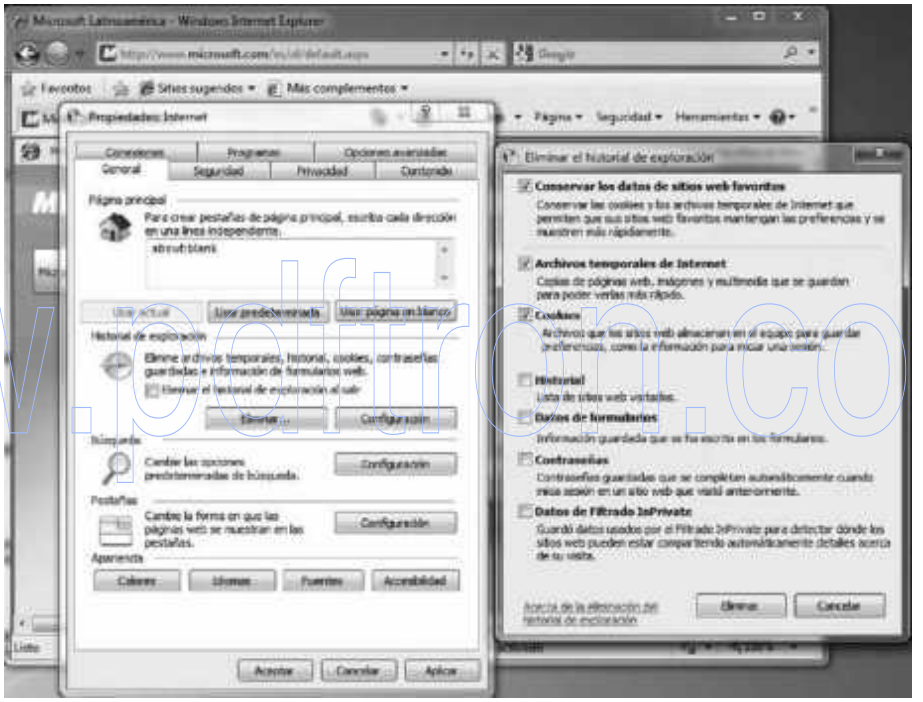
→ Borrar las Cookies en Internet Explorer 8

PREPÁRESE. Para borrar cookies, lleve a cabo estos pasos:

1. Abra **Internet Explorer**.
2. Dé clic en el botón de **Herramientas**, y después dé clic en **Opciones de Internet**.
3. En la ficha **General**, bajo **Historial de Exploración**, dé clic en **Eliminar**. Vea la Figura 5-8.
4. Seleccione el recuadro de selección **Cookies**, y después dé clic en **Eliminar** si no se ha seleccionado aún. Retire la selección o seleccione los recuadros de selección para cualquier otra información que también desee borrar. Si desea conservar las cookies de sus favoritos guardados, seleccione el recuadro de selección de datos de sitios Web Conservar Favoritos.

Figura 5-8

Cómo borrar cookies y archivos temporales



Estar consciente de cómo se usa su información privada cuando se explora la Web es también importante para ayudarle a prevenir publicidad enfocada, fraudes e identificar robos. Aquí, es importante usar las configuraciones apropiadas de privacidad.

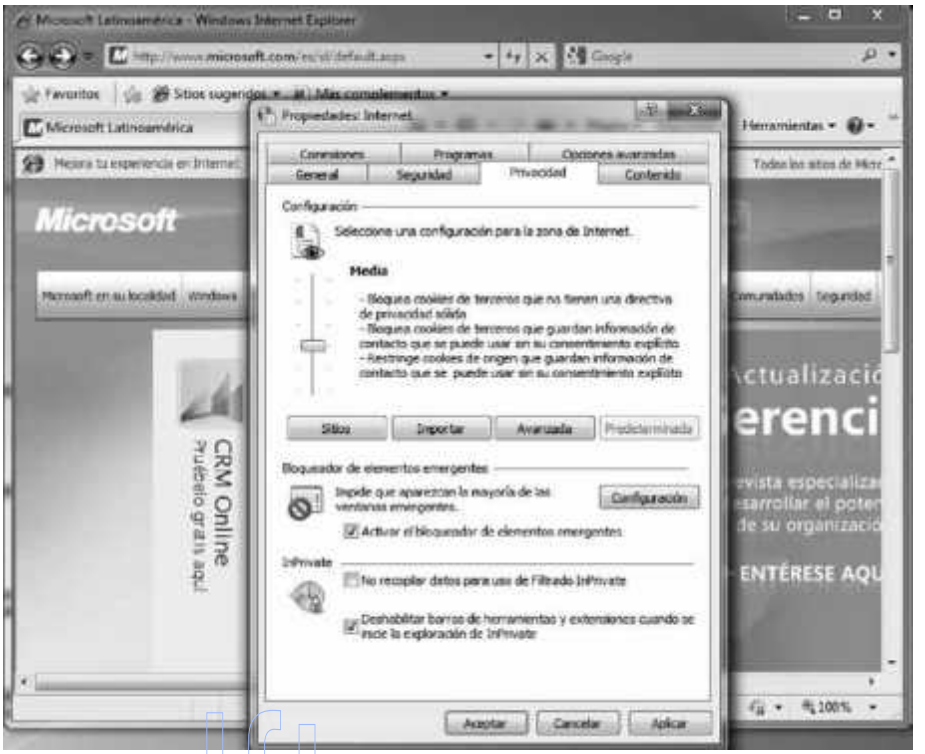
→ Cambiar las Configuraciones de Privacidad

PREPÁRESE. Para cambiar las configuraciones de privacidad de Internet Explorer, lleve a cabo estos pasos:

1. Abra **Internet Explorer**.
2. Dé clic en el botón **Herramientas**, y después dé clic en **Opciones de Internet**.
3. Dé clic en la ficha **Privacidad**. Vea la Figura 5-9.

Figura 5-9

Ficha de Privacidad



Para ajustar sus configuraciones de seguridad, ajuste la barra de deslizamiento a una nueva posición en la escala de privacidad. El nivel predeterminado es Medio; se recomienda que configure sus configuraciones en Medio o más alto. Si da clic en el botón Avanzadas, puede controlar ciertas configuraciones, y si da clic en el botón Editar, puede permitir o bloquear cookies de sitios Web individuales.

Las ***ventanas emergentes*** son muy comunes en Internet. Aunque algunas ventanas emergentes son controles útiles de un sitio Web, la mayoría son simples anuncios publicitarios molestos, y unos cuantos pueden intentar cargar spyware u otros programas maliciosos. Para proteger su computadora, Internet Explorer tiene la capacidad de suprimir algunas o todas las ventanas emergentes. Para configurar el bloqueador de ventanas emergentes, use el siguiente procedimiento:

→ Configurar el Bloqueador de Ventanas Emergentes

PREPÁRESE. Inicie sesión en Windows 7, y después lleve a cabo estos pasos:

1. Dé clic en **Inicio,** y dé clic en **Panel de Control**. Aparecerá la ventana de **Panel de Control**.
2. Seleccione **Redes e Internet** y después **Opciones de Internet**. Aparecerá la página de **Propiedades de Internet**.
3. Dé clic en la pestaña **Privacidad**. Asegúrese de que la opción **Activar Bloqueador de Elementos Emergentes** esté seleccionada.
4. Dé clic en **Configuraciones**. Aparecerá el cuadro de diálogo de **Configuraciones de Bloqueador de Elementos Emergentes**.

5. Para permitir las ventanas emergentes de un sitio Web específico, escriba la dirección del sitio en el recuadro de texto **Dirección de sitio Web para permitir** y dé clic en **Agregar**. Repita el proceso para agregar sitios adicionales a la lista de sitios Permitidos.
6. Ajuste la lista desplegable de niveles de Bloqueo en una de las siguientes configuraciones:
   - **Alto**: Bloquea todas las ventanas emergentes
   - **Medio**: Bloquea la mayoría de las ventanas emergentes automáticas
   - **Bajo**: Permite las ventanas emergentes de sitios seguros
7. Dé clic en **Cerrar** para cerrar el cuadro de diálogo de Configuraciones del Bloqueador de Elementos Emergentes.
8. Dé clic en **OK** para cerrar la página de **Propiedades de Internet**.

▶ *Cómo Examinar las Zonas de Contenido*

Para ayudarse a administrar la seguridad al visitar sitios, Internet Explorer divide su conexión de red en cuatro ***zonas*** o tipos ***de contenido.*** Para cada una de estas zonas, está asignado un nivel de seguridad.

La seguridad para cada zona es asignada con base en los peligros asociados con la zona. Por ejemplo, se supone que cuando se conecta a un servidor en su propia corporación, está más seguro que cuando se conecta a un servidor en Internet.

Las cuatro zonas predeterminadas de contenido son las siguientes:

- **Zona de Internet**: Esta zona es usada para todo lo que no esté asignado a otra zona y a nada más que no esté en su computadora o en la red de su organización (intranet). El nivel predeterminado de seguridad de la zona de Internet es Medio.
- Zona de intranet local: Esta zona es usada para sitios que son parte de la red de una organización (intranet) y que no requieren de un servidor proxy, según las definiciones del administrador del sistema. Estos incluyen sitios especificados en la ficha de Conexiones, la red, trayectorias como \\nombre de PC\nombre de carpeta, y sitios de la intranet local como http://interno. Puede agregar sitios a esta zona. El nivel predeterminado de seguridad para la zona de intranet Local es Medio-Bajo, lo que significa que Internet Explorer permitirá que todas las cookies de los sitios Web en esta zona sean guardadas en su computadora y que sean leídas por el sitio Web que las creó. Finalmente, si el sitio Web requiere de NTLM o autenticación integrada, este usará automáticamente su nombre de usuario y contraseña.
- Zona de sitios de confianza: Esta zona contiene sitios desde los que cree que puede descargar o ejecutar archivos sin dañar su sistema. Puede asignar sitios a esta zona. El nivel predeterminado de seguridad para la zona de sitios De Confianza es Bajo, lo que significa que Internet Explorer permitirá que todas las cookies de los sitios Web en esta zona sean guardados en su computadora y que sean leídos por el sitio Web que las creó.
- Zona de sitios restringidos: Esta zona contiene sitios en los que no confía y desde los que descargar o ejecutar archivos podría dañar su computadora o sus datos. Estos sitios son considerados un riesgo de seguridad. Puede asignar sitios a esta zona. El nivel predeterminado de seguridad para la zona de sitios Restringidos es Alto, lo que significa que Internet Explorer bloqueará todas las cookies de los sitios Web en esta zona.

Para decidir en qué zona cae una página Web, observe el lado derecho de la barra de estado de Internet Explorer.

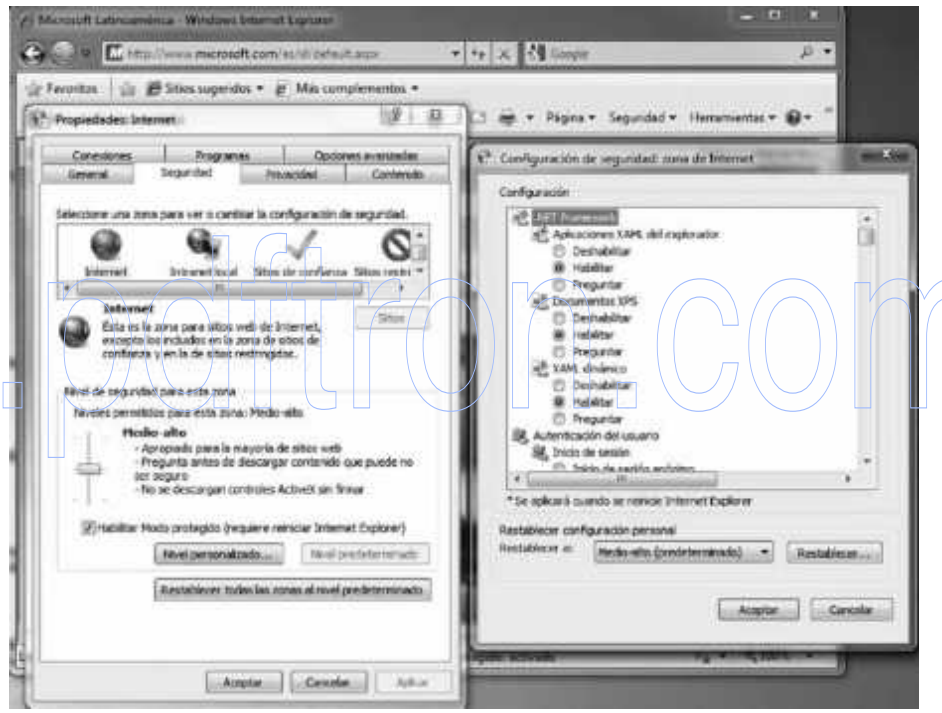
→ Nivel de Seguridad para la Zona de Contenido Web

PREPÁRESE. Para modificar el nivel de seguridad para una zona de contenido Web, lleve a cabo estos pasos:

1. Dé clic en el botón **Herramientas**, y después seleccione **Opciones de Internet**.
2. En el cuadro de diálogo de **Opciones de Internet**, en la ficha de **Seguridad**, dé clic en la zona en la que desea establecer el nivel de seguridad. Vea la Figura 5-10.
3. Arrastre la barra de deslizamiento para establecer el nivel de seguridad en **Alto**, **Medio**, o **Bajo**. Internet Explorer describe cada opción para ayudarle a decidir qué nivel elegir. Se le pedirá confirmar cualquier reducción en el nivel de seguridad. También podrá elegir el botón de **Nivel Personalizado** para un control más detallado.
4. Dé clic en **OK** para cerrar el cuadro de diálogo de **Opciones de Internet**.

Figura 5-10

Cómo configurar las zonas de contenido de seguridad



Para cada una de las zonas de contenido Web, existe un nivel predeterminado de seguridad. Los niveles de seguridad disponibles en Internet Explorer son los siguientes:

- **Alto**: Excluye cualquier contenido que pueda dañar su PC
- Medio: Le advierte antes de ejecutar contenido potencialmente dañino
- Bajo: No le advierte antes de ejecutar contenido potencialmente dañino
- Personalizado: Una configuración de seguridad de su propio diseño

La manera más fácil de modificar la configuración de seguridad que Internet Explorer impone sobre un sitio Web específico es agregar manualmente el sitio a una zona de seguridad. El procedimiento usual es agregar un sitio a la zona de sitios De Confianza para incrementar sus privilegios, o en vez de ello agregarlo a la zona de sitios Restringidos para reducir sus privilegios. Para hacer esto, use el siguiente procedimiento:

→ Agregar un Sitio a una Zona de Seguridad

PREPÁRESE. Inicie sesión en Windows 7, y después lleve a cabo estos pasos:

1. Dé clic en **Inicio**, y seleccione **Panel de Control**. Aparecerá la ventana del Panel de Control.
2. Seleccione **Redes e Internet** y después **Opciones de Internet**. Aparecerá la página de Propiedades de Internet.
3. Dé clic en la pestaña **Seguridad**.
4. Seleccione ya sea la zona de **Sitios de Confianza** o **Sitios Restringidos** a la cual desee agregar un sitio.
5. Dé clic en **Sitios**. Aparecerá el cuadro de diálogo de Sitios de Confianza o Sitios Restringidos.
6. Escriba la dirección del sitio Web que desee agregar a la zona en el cuadro de texto **Agregar este sitio Web a la zona**, y dé clic en **Agregar**. Aparecerá la dirección en la lista de sitios Web.
7. Dé clic en **Cerrar** para cerrar el cuadro de diálogo de Sitios de Confianza o Sitios Restringidos.
8. Dé clic en **OK** para cerrar la página de Propiedades de Internet.

Para modificar las propiedades de seguridad de una zona, use el siguiente procedimiento:

→ Modificar las Configuraciones de una Zona de Seguridad

PREPÁRESE. Inicie sesión en Windows 7, y después lleve a cabo estos pasos:

1. Dé clic en **Inicio**, y elija **Panel de Control**. Aparecerá la ventana del Panel de Control.
2. Seleccione **Redes e Internet** y después **Opciones de Internet**. Aparecerá la página de Propiedades de Internet.
3. Dé clic en la ficha **Seguridad**.
4. Seleccione la zona para la cual desea modificar las configuraciones de seguridad.
5. En el cuadro de **Nivel de seguridad para esta zona**, ajuste la barra de deslizamiento para incrementar o disminuir el nivel de seguridad para la zona. Al mover la barra de deslizamiento hacia arriba se incrementa la protección para la zona, y al mover la barra de deslizamiento hacia abajo se disminuye.
6. Seleccione o retire la selección del recuadro de selección **Activar modo protegido**, si lo desea.
7. Para ejercer un control más preciso sobre las configuraciones de seguridad de la zona, dé clic en **Nivel personalizado**. Aparecerá el cuadro de diálogo de Configuraciones de Seguridad para la zona.
8. Seleccione los botones de selección para las configuraciones individuales en cada una de las categorías de seguridad. Los botones de selección usualmente hacen posible activar una configuración, desactivarla, o avisar al usuario antes de activarla.
9. Dé clic en **OK** para cerrar el cuadro de diálogo de Configuraciones de Seguridad.
10. Dé clic en **OK** para cerrar la página de Propiedades de Internet.

Phishing y Pharming

Phishing y pharming son dos formas de ataque usados para atraer con engaños a los individuos a sitios Web fraudulentos en un intento por diseminar malware o recopilar información personal.

Phishing es una técnica basada en ingeniería social. Con el phishing, se les pide a los usuarios (normalmente a través de correos electrónicos o sitios Web) suministrar información personal en una de dos maneras:

- Contestando a un correo electrónico en que se les pregunte su nombre de usuario, contraseña y otra información personal, como números de cuenta, PINs y números de Seguro Social.
- Navegando a un sitio Web que parece convincente que les incita a suministrar su información personal, como contraseñas y números de cuenta.

Por ejemplo, digamos que recibe un correo electrónico diciéndole que la cuenta de su tarjeta de crédito acaba de expirar o que necesita validar su información. El correo electrónico le ofrece un vínculo al que acceder dando clic. Cuando da clic en el vínculo, accede a un sitio Web falso. Sin embargo, al "iniciar sesión" en el sitio con su información real, de hecho estará proveyendo su nombre de usuario y contraseña al hacker, que después podrá usar esta información para acceder a su cuenta.

Para ayudarle a protegerse contra el phishing, Internet Explorer 8 incluye el Filtro SmartScreen, el cual examina el tráfico en busca de evidencia de actividad de phishing y muestra una advertencia al usuario si encuentra alguna. Este también envía la dirección de regreso al servicio de SmartScreen de Microsoft para realizar una comparación contra las listas de sitios conocidos de phishing y malware. Si el Filtro SmartScreen descubre que un sitio Web que está visitando está en la lista de sitios conocidos de malware o phishing, Internet Explorer mostrará una página Web de bloqueo y la barra de Dirección aparecerá en rojo. Desde la página de bloqueo, puede elegir evadir el sitio Web bloqueado e ir a su página de inicio, o puede continuar su ingreso al sitio Web bloqueado, aunque esto no se recomienda. Si decide continuar su ingreso al sitio Web bloqueado, la barra de Dirección continuará apareciendo en rojo.

Una de las mejores maneras de evitar dichas tácticas es saber que existen. Consecuentemente, cuando reciba un correo electrónico que le solicite información personal, busque señales de que el correo electrónico es falso y que los vínculos dentro de este le llevan a sitios fraudulentos (por ejemplo, en vez de entrar en ebay.com, un vínculo ingresa a ebay.com.com o a ebay_ws-com). No confíe en hipervínculos. Nunca suministre una contraseña u otra información confidencial a un sitio Web a menos de que mismo escriba la dirección y esté seguro de que es correcta.

Pharming es un ataque enfocado en redirigir el tráfico de un sitio Web a un sitio Web fraudulento. Esto normalmente se logra cambiando el archivo del servidor (un texto que provee la resolución del nombre para nombres de servidores o dominios a la dirección IP) en una computadora o explotando una vulnerabilidad en un servidor DNS. Para protegerse contra pharming, necesita asegurarse de que su sistema cuenta con los parches de seguridad más actuales y que cuenta con un paquete de software de antivirus actualizado. Además, UAC le ayuda a proteger el archivo del servidor, ya que este se localiza en la carpeta System32, que es una de las áreas que UAC ayuda a proteger.

▪ Cómo Proteger Su Servidor

↓ EN RESUMEN

Al considerar la seguridad, recuerde que necesita asegurar su red, a sus clientes y sus servidores. Al asegurar estos tres, adopta un método en niveles que hace más difícil que los hackers y el malware violen su organización. En las lecciones anteriores, hablamos sobre cómo mantener su red segura. Anteriormente en esta lección, hablamos sobre cómo mantener a sus clientes seguros. Ahora, en esta parte de la lección, nos enfocaremos en cómo asegurar el servidor.

☑ Listo para la Certificación

¿Sabe cómo proteger sus servidores de manera que siempre estén funcionando adecuadamente? —4.3

Como ya sabe, los servidores son computadoras cuyo objetivo es brindar servicios y aplicaciones de red para su organización. A diferencia de una estación de trabajo, si un servidor falla, esto afectará a múltiples usuarios. Por lo tanto, es importante mantener a un servidor más seguro que a una estación de trabajo.

▶ *Cómo Colocar el Servidor*

El primero paso para asegurar un servidor es determinar dónde colocarlo. Desde luego, el servidor debe ser mantenido en una ubicación segura. Además, los servidores deben estar en su propia subred y VLAN para reducir el tráfico que llega a ellos, incluyendo transmisiones.

En algunos casos, puede requerir colocar los servidores en una oficina subsidiaria. En situaciones en las que necesite instalar un controlador de dominio en un ambiente de seguridad física baja, deberá considerar instalar un Controlador de Dominio de Sólo Lectura (RODC) que contiene una copia no editable del Directorio activo y redirige todos los intentos de escritura a un Controlador de Dominio Total. Este dispositivo duplica todas las cuentas, excepto aquellas sensibles. Por lo tanto, si el controlador de dominio está comprometido, los atacantes son limitados en lo que pueden hacer al escribir información en Directorio activo.

▶ *Cómo Fortalecer al Servidor*

El siguiente paso en la seguridad de un servidor es fortalecerlo para reducir la superficie del ataque, reduciendo así las vulnerabilidades del servidor. Para fortalecer a un servidor, deberá buscar los lineamientos y mejores prácticas en seguridad para servidores de Windows y los servicios específicos de red que esté instalando, como Microsoft Exchange o Microsoft SQL Server.

Uno de los pasos más importantes en la seguridad de un servidor es verificar que Windows, las aplicaciones de Microsoft y otras aplicaciones de red sean mantenidas actuales con los parches de seguridad más novedosos. Como con los clientes, puede hacer esto usando Windows Updates, WSUS y SCCM. Desde luego, antes de aplicar parches a un sistema de producción, asegúrese de comprobar las actualizaciones de seguridad.

Para reducir la superficie de ataque de un servidor, deberá desactivar cualquier servicio que no sea necesario, de modo que ese servicio no pueda ser explotado en el futuro. Además, deberá considerar usar firewalls de servidores (como Firewall de Windows), que bloqueará todos los puertos que no estén siendo usados.

Para reducir el efecto de pérdida de un servidor, deberá separar los servicios. ¡Nunca instale todos sus servicios en un solo servidor! También necesita planear el resto y esperar lo mejor. Esto significa que necesita anticipar que un servidor fallará eventualmente. Por lo tanto, debe considerar usar suministros de energía redundante, discos RAID (Conjunto Redundante de Discos Independientes, por sus siglas en inglés), tarjetas de red redundante y clústers.

También deberá desactivar o borrar cualquier cuenta innecesaria. Por ejemplo, aunque no pueda borrar la cuenta de administrador, puede cambiarle el nombre a algo más de modo que sea más difícil para un hacker adivinarlo. Además, no deberá usar la cuenta de administrador para todo. Por ejemplo, si debe ejecutar un servicio específico, cree una cuenta de servicio para ese servicio y otórguele los derechos y permisos mínimos que necesite para ejecutarse. Desde luego, la cuenta de invitado debe ser desactivada.

Además de desactivar o borrar cualquier cuenta innecesaria y únicamente asignar los derechos y permisos mínimos necesarios para que los usuarios hagan su trabajo, también deberá minimizar quién puede iniciar sesión localmente en el servidor.

Adicionalmente, deberá desactivar cualquier protocolo de autenticación no seguro. Por ejemplo, no deberá usar un Protocolo de Autenticación de Contraseñas (PAP) al usar protocolos de acceso remoto. No deberá usar FTP con contraseñas. En vez de esto, use un anónimo que no requiera de contraseñas (suponiendo que su contenido no necesite ser seguro) o use FTP seguro, que encriptará la contraseña y el contenido cuando esté siendo transmitido sobre la red. Por razones similares no deberá usar telnet. En vez de esto, use SSH (Secure Shell).

Finalmente, deberá habilitar una fuerte política de auditoría e inicio de sesión y revisar estos registros en una base regular. Si alguien intenta atacar un servidor o hacer algo que no debería estar haciendo, tendrá un registro de las actividades de esa persona. Esto deberá incluir inicios de sesión de cuentas exitosos y fallidos.

Microsoft Baseline Security Analyzer (MBSA, Analizador de Seguridad Básica de Microsoft) es una herramienta de software puesta en circulación por Microsoft para determinar el estado de seguridad de un sistema evaluando las actualizaciones faltantes en seguridad y las configuraciones de seguridad menos seguras dentro de los componentes de Microsoft Windows como Internet Explorer, el servidor Web IIS, y productos como Microsoft SQL Server y las configuraciones de macros de Microsoft Office. Vea la Figura 5-11.

Figura 5-11

Analizador de Seguridad Básica de Microsoft

Microsoft frecuentemente publica guías de seguridad y guías de las mejores prácticas para diversos productos. Además, Microsoft ha publicado las Amenazas y Contramedidas (Configuraciones de Seguridad en Windows Server 2008 y Windows Vista), que pueden encontrarse en http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=037d908d-6a1c-4135-930c-e3a0d6a34239.

← Cómo Asegurar DNS Dinámico

Desde Windows Server 2003, los servidores de Windows han provisto de soporte para la funcionalidad de actualizaciones dinámicas de DNS. DNS Dinámico permite que las computadoras de los clientes actualicen dinámicamente sus registros de recursos en DNS. Cuando use esta funcionalidad, mejorará la administración de DNS reduciendo el tiempo que le toma administrar manualmente los registros de zonas de DNS. Puede usar la funcionalidad de actualizaciones de DNS con DHCP para actualizar los registros de recursos cuando se cambie la dirección IP de una computadora.

Con actualizaciones típicas dinámicas no aseguradas, cualquier computadora puede crear registros en su servidor DNS, lo que lo deja abierto a actividad maliciosa. Para proteger su servidor DNS, asegúrelo de modo que únicamente miembros de un dominio de Directorio activo puedan crear registros en el servidor.

Matriz de Habilidades de Resumen

En esta lección aprendió:

- Debido a que las computadoras de los clientes están conectadas a la red de una organización y pueden tener acceso directo e indirecto a los servidores y a los recursos de red, es importante que estas computadoras sean protegidas.
- Un virus es un programa que se puede copiar a sí mismo e infectar una computadora sin aprobación o conocimiento del usuario.
- Una backdoor en un programa otorga control remoto y no autorizado de un sistema o inicia una tarea no autorizada.
- Algunos virus, gusanos, rootkits, spyware y adware trabajan explotando las brechas de seguridad en Windows, Internet Explorer o Microsoft Office.
- El primer paso para protegerse mismo en contra de malware es mantener su sistema Windows (así como otros productos de Microsoft, como Internet Explorer y Microsoft Office) actualizado con los últimos paquetes de servicio, parches de seguridad y otras reparaciones críticas.
- Una falsa alarma de virus es un mensaje que advierte al receptor sobre una amenaza no existente de virus informático, enviado normalmente como un correo electrónico cadena que le dice al receptor que lo reenvíe a todos los que conozca. Esta es una forma de ingeniería social que juega con la ignorancia y el miedo de las personas.
- Control de Cuentas de Usuario (UAC) es una característica que ayuda a prevenir malware. UAC fue introducida primero con Windows Vista y está incluida con Windows 7.
- Microsoft recomienda que siempre use el Firewall de Windows.
- Los archivos offline no son encriptados a menos que elija que así sea. Puede optar por encriptar sus archivos offline si estos contienen información sensible o confidencial y desea hacerlos más seguros restringiendo el acceso a ellos.
- Si no permite que los usuarios inicien sesión como administradores, puede limitar qué software instalan estos usuarios y puede proteger mejor el sistema de malware.
- También puede usar Políticas Grupales para restringir qué software puede ser ejecutado en la computadora de un cliente.
- La mayoría de los correos electrónicos son no solicitados; dichos mensajes son llamados spam o correo electrónico basura.
- El mejor lugar para establecer un sistema de filtrado de spam es en la transferencia de correo electrónico en un servidor o dispositivo dedicado, o como parte de un dispositivo o servicio de firewall.
- Para hacer que un mensaje spam se vea como un mensaje legítimo, algunas veces los spammers intentan falsificar una dirección de correo electrónico o dirección IP de donde viene un mensaje.
- Los spammers buscan servidores SMTP no protegidos para transferir sus correos electrónicos a través de ellos.
- Aunque algunas ventanas emergentes son controles útiles de sitios Web, la mayoría son simplemente anuncios publicitarios molestos, y unos cuantos intentan cargar spyware u otros programas maliciosos.
- Para ayudarle a administrar la seguridad al visitar sitios Web, Internet Explorer divide su conexión de red en cuatro zonas o tipos de contenido. Cada una de estas zonas tiene asignado un nivel de seguridad.
- Phishing y pharming son dos formas de ataque usados para atraer con engaños a los individuos a sitios Web fraudulentos en un intento por diseminar malware o recolectar información personal.

- Todos los servidores deben ser mantenidos en una ubicación segura. Además, los servidores deben estar en su propia subred y VLAN para reducir el tráfico que llega a ellos, incluyendo transmisiones.
- También debe asegurar un servidor fortaleciéndolo para reducir la superficie de ataque. Al fortalecer un servidor, busque guías de seguridad y las mejores prácticas para servidores de Windows, así como los servicios específicos de red que está instalando.
- Para asegurar su servidor DNS, hágalo de tal modo que únicamente los miembros de un dominio de Directorio activo puedan crear registros en el servidor DNS.

» Evaluación de Conocimiento

Opción Múltiple

Encierre en un círculo la letra que corresponda a la mejor respuesta.

1. ¿Qué tipo de malware se copia a sí mismo sobre otras computadoras sin la aprobación del propietario y con frecuencia borrará o corromperá archivos?
   a. Virus
   b. Gusano
   c. Troyano
   d. Spyware
2. ¿Qué tipo de malware recopila información personal o historiales de exploración, con frecuencia sin el conocimiento del usuario?
   a. Virus
   b. Gusano
   c. Troyano
   d. Spyware
3. Su computadora parece estar lenta y nota que tiene una página Web predeterminada diferente a la usual. ¿Cuál es la causa más probable de problemas?
   a. Su ISP ha disminuido la velocidad de su conexión de red.
   b. Su computadora ha sido infectada con malware.
   c. No actualizó su computadora.
   d. Accidentalmente dio clic al botón de turbo.
4. Además de instalar un paquete de software de antivirus, siempre debe _____ para proteger su computadora contra malware.
   a. mantener su máquina actualizada con los últimos parches de seguridad
   b. reiniciar su computadora con regularidad
   c. cambiar su contraseña con regularidad
   d. falsificar su dirección IP
5. Un conjunto acumulativo cabalmente comprobado de hotfixes y otros parches es conocido como:
   a. una actualización recomendada.
   b. un paquete de hotfixes.
   c. un paquete de servicio.
   d. una actualización crítica.

6. ¿Qué tecnología usa Windows para prevenir cambios no autorizados en su sistema?
   a. UAC
   b. Modo protegido
   c. Windows Defender
   d. ProtectGuard
7. Al usar UAC, ¿cuál de los siguientes requiere permisos o derechos administrativos?
   a. Instalación de actualizaciones desde Windows Update
   b. Cambio de la fecha y hora
   c. Restauración del adaptador de red
   d. Instalación de controladores desde Windows Update o adjuntos con el sistema operativo
8. ¿Qué mecanismo está trabajando cuando intenta cambiar las configuraciones de pantalla de una computadora y aparece una ventana emergente preguntando si desea continuar?
   a. Firewall de Windows
   b. Modo Protegido
   c. Windows Update
   d. UAC
9. ¿Qué software de firewall en el servidor viene con versiones actuales de Windows?
   a. Firewall de Windows
   b. Modo Protegido de Windows
   c. UAC
   d. Windows GuardIt
10. ¿Qué programa usaría para configurar IPsec en una computadora que ejecuta Windows Server 2008?
    a. Firewall de Windows con Plugin de IPsec
    b. Monitor IPsec
    c. Windows con Seguridad Avanzada
    d. Consola de Configuración de IPsec
11. Si tiene información sensible o confidencial almacenada en sus archivos fuera de línea, se recomienda que:
    a. Elimine su caché.
    b. Encripte los archivos fuera de línea.
    c. Elimine sus cookies.
    d. Ejecute ipconfig /renewip.
12. Determina que correos electrónicos legítimos están siendo bloqueados por su dispositivo de bloqueo de spam. ¿Qué debe hacer?
    a. Eliminar los elementos en cuarentena
    b. Reiniciar el dispositivo de bloqueo de spam
    c. Agregar la dirección o el dominio para estos correos electrónicos a la lista blanca
    d. Agregar la dirección o el dominio para estos correos electrónicos a la lista negra

13. SMTP usa el puerto TCP:
    a. 43.
    b. 25.
    c. 80.
    d. 443.
14. ¿Cuántas zonas de contenido existen en Internet Explorer?
    a. 1
    b. 2
    c. 4
    d. 8
15. Digamos que recibe un correo electrónico que dice que su cuenta acaba de expirar y le pide que inicie sesión en un sitio Web que parece legítimo para arreglar el problema. Este es el ejemplo más probable de:
    a. phishing.
    b. pharming.
    c. phaking.
    d. falsificación/spoofing de direcciones IP.

Llene el Espacio en Blanco

Complete las siguientes oraciones escribiendo la palabra o palabras correctas en los espacios en blanco provistos.

1. _____ es software que está diseñado para infiltrarse en o infectar una computadora, normalmente con malas intenciones.
2. Un _____ es un programa auto-copiante que se copia a sí mismo a otras computadoras mientras que consume recursos de red.
3. El programa antispyware de Microsoft se llama _____.
4. Para que un software de antivirus sea efectivo, debe ser mantenido _____.
5. Un ejemplo de _____ es un mensaje que le dice que borre el archivo win.com porque es un virus.
6. Si desea controlar qué actualizaciones son impuestas a los clientes dentro de su organización, usaría _____ o _____.
7. _____ es cuando se le pregunta si desea continuar con una acción y su escritorio es opacado y otros programas son detenidos temporalmente hasta que aprueba el cambio.
8. _____ son copias de archivos de red que son almacenados en su computadora de modo que pueda acceder a ellos cuando no esté conectado a la red.
9. _____ es otro nombre para correo electrónico basura.
10. _____ es un sistema de validación de correos electrónicos que está diseñado para verificar que un correo electrónico está llegando desde un servidor apropiado de correos electrónicos.

» Evaluación de Competencia/Capacidad

Escenario 5-1: Revisión de Seguridad Física

Acaba de ser contratado como administrador TI para la Compañía ABC. Al otro lado de su escritorio está una mesa con siete servidores físicos. Se acerca a su jefe y le pregunta por qué los servidores están afuera y no bajo llave. Él dice que están colocados en la mesa de modo que puedan ser monitoreados y observados fácilmente. ¿Cómo debería responder a su jefe?

Escenario 5-2: Programación de Puertas Traseras

Ha sido contratado como consultor de seguridad para una Corporación Costosa. Un día, está trabajando con el Jefe de Servicios de Información en una nueva política de seguridad integral para la compañía. Aunque el Jefe de Servicios de Información no es un programador, desea comprender cómo puede evitar que los programadores creen una back door en los programas que ellos crean para la compañía. ¿Qué le diría?

» Evaluación de Destreza

Escenario 5-3: Exploración con el Analizador de Seguridad Básica de Microsoft

Descargue e instale la versión más actual del Analizador de Seguridad Básica de Microsoft en un servidor de Windows, y después explore la computadora en busca de actualizaciones de seguridad faltantes y configuraciones de seguridad menos óptimas.

Escenario 5-4: Observación de Windows Updates

Vaya a http://www.microsoft.com/technet/security/bulletin/advance.mspx. Lea la notificación de avances más recientes o el resumen de boletines de seguridad más recientes y revise el resumen ejecutivo. Determine cuántos boletines de seguridad existen para el mes más reciente. Después, ejecute Windows Update para actualizar su sistema con los parches más recientes.

Área de Trabajo Lista

→ Cómo Mantener el Paso con la Seguridad

Administrar/mantener la seguridad para una organización frecuentemente es un trabajo de tiempo completo que normalmente requiere a múltiples personas con diversos conjuntos de habilidades. Por ejemplo, puede contar con una persona que sea responsable de los enrutadores/routers y firewalls, otra persona que sea responsable de los servidores y otra persona que sea responsable de las computadoras de los clientes. También puede tener un gerente de seguridad que supervise todos los elementos relacionados con la seguridad, incluyendo la seguridad física. Desde luego, el Director Ejecutivo, el Jefe de Servicios de información y otros ejecutivos de una compañía son los responsables finales de la seguridad.

Sin embargo, para que la seguridad sea efectiva, debe recordar que todos necesitan participar. Esto incluye a los ejecutivos que dan soporte al departamento de TI y ayudan a implementar y a dar soporte a las decisiones relacionadas con la seguridad, así como a los miembros del personal de TI que establecen las medidas de seguridad y las monitorean. Pero no olvide que el vínculo más débil puede ser el usuario final. Las mejores prácticas, la capacitación de consciencia, y los recordatorios constantes son clave para comunicar a todos los empleados porqué la seguridad es tan importante.