Capítulo 5

Vulnerabilidades y amenazas

OBJETIVOS DE CERTIFICACIÓN

Ser capaz de identificar diferentes áreas de amenaza para un sistema es una habilidad importante para tener como profesional de seguridad y una que seguramente se pondrá a prueba para el examen de certificación Security +. Este capítulo identificará los tipos populares de amenazas contra diferentes tipos de dispositivos y sistemas, así como los diferentes tipos de software malicioso con los que debe estar familiarizado para el examen.

OBJETIVO DE CERTIFICACIÓN 5.01

Problemas de seguridad con vulnerabilidades

Antes de entrar en los diferentes tipos de amenazas a un sistema, hablemos de algunas razones por las que los sistemas son vulnerables y el impacto que un sistema vulnerable tiene para una organización. En el capítulo 2 se le presentó el término *vulnerabilidad,* que es una debilidad en un producto o sistema. En este capítulo aprenderá más acerca de por

qué existen esas vulnerabilidades y qué puede hacer para reducir el número de vulnerabilidades en un sistema.

Este capítulo se centra principalmente en las vulnerabilidades encontradas en sistemas que están "en las instalaciones" (es decir, en su LAN) frente a los sistemas o aplicaciones en la nube. Si su organización utiliza recursos en la nube, asegúrese de evaluar también los tipos de vulnerabilidades que existen en la nube.

Un tipo muy importante de vulnerabilidad a tener en cuenta es una vulnerabilidad *de día cero*, que es una vulnerabilidad desconocida para el proveedor de software que creó el software y, como resultado, aún no se ha creado ninguna solución o parche para la vulnerabilidad. Una vulnerabilidad de día cero es susceptible a un ataque de día cero, que es un tipo de ataque muy peligroso porque el software aún no ha sido parcheado.

Para ayudar a prevenir ataques de día cero, use una combinación de controles de seguridad, incluidos los sistemas de parches y las aplicaciones de forma regular, el uso de firewalls de capa de aplicación para controlar el tipo de tráfico que puede llegar a un sistema o aplicación, y la implementación de un sistema de prevención de intrusiones (IPS) para supervisar la actividad, identificar amenazas y bloquear ataques.

Razones para los sistemas vulnerables

Hay un gran número de vulnerabilidades, o debilidades, en un sistema que permiten a un atacante obtener acceso al sistema y sus datos. En esta sección, aprenderá sobre las vulnerabilidades más comunes en un sistema.

Configuraciones débiles

La primera razón para un sistema vulnerable es la configuración débil. La configuración débil de un sistema viene en muchas formas diferentes, siendo los siguientes los errores de configuración más comunes:

■ **Permisos abiertos** No configurar permisos en un sistema o en una aplicación puede dejar el sistema abierto a los atacantes. Es fundamental asegurarse de que las cuentas de invitado o anónimas no tengan acceso de escritura a los datos del sistema.

■ **Cuentas raíz no seguras** Se deben seguir las mejores prácticas con cuentas de administrador, como la cuenta raíz en Linux y la cuenta de administrador en Windows. Las prácticas recomendadas comunes incluyen cambiar el nombre de la cuenta predeterminada, establecer una contraseña segura en la cuenta y limitar la creación de cuentas adicionales de nivel raíz.

■ **Errores** Los errores son errores cometidos en la configuración que podrían dejar el sistema abierto a ataques. Por ejemplo, no limitar las transferencias de zona en un servidor DNS podría dejar los datos DNS abiertos para el atacante.

■ **Cifrado débil** No cifrar los datos en reposo y los datos en tránsito es un error crítico. Con todos los dispositivos, aplicaciones y protocolos, busque cómo se pueden cifrar los datos para proteger la confidencialidad de los datos de la empresa y garantizar que el algoritmo de cifrado que se utiliza se considere un algoritmo sólido según los estándares actuales. Por ejemplo, aprenderá sobre los algoritmos de cifrado en el **Capítulo 12** y el hecho de que DES y 3DES se consideran protocolos de cifrado débiles. Si una aplicación utiliza DES o 3DES, debería ver si puede cambiar la configuración y utilizar el algoritmo AES más seguro. Consulte **los capítulos 12** y **13** para obtener más información sobre el cifrado.

■ **Protocolos no seguros** Asegúrese de que las aplicaciones utilizan versiones seguras de protocolos para que la comunicación esté cifrada. Por ejemplo, asegúrese de que una aplicación web usa HTTPS en lugar de HTTP.

- **Configuración** predeterminada Revise la configuración predeterminada de un sistema o aplicación y busque la configuración predeterminada que pueda poner en riesgo el sistema. Por ejemplo, las versiones anteriores de Windows Server tenían instalado el software de servidor web de Microsoft de forma predeterminada. Esto significaba que su Windows Server estaba abierto a ataques web listos para usar. Como administrador, se le enseñó a eliminar el software del servidor web después de la instalación de Windows si no necesitaba el software del servidor web.

- **Puertos y** servicios abiertos Asegúrese de limitar los servicios que se ejecutan en un sistema, lo que reduce los puertos que están abiertos en un sistema.

Riesgos de terceros

También existen riesgos al trabajar con compañías de terceros. Las acciones realizadas por empresas de terceros con las que trabaja pueden dejar a su empresa vulnerable. Los siguientes son algunos ejemplos:

- **Gestión de proveedores** La forma en que un proveedor administra sus productos puede presentar vulnerabilidades en su entorno que utiliza los productos de ese proveedor. Por ejemplo, ¿cómo se integra el sistema de un proveedor en su red? ¿Utiliza protocolos seguros? ¿Necesita una cuenta en la red? Si un producto es más antiguo, es posible que el proveedor ya no admita el producto. Un producto que ya no es compatible ya no tiene parches creados, lo que significa que podría estar abierto a ataques de día cero.

- **Cadena de suministro** Si está trabajando con un proveedor que no sigue las mejores prácticas de seguridad, podría recibir un producto del proveedor que se ha visto comprometido y luego conectarse a su red.

- Desarrollo de código **subcontratado El código** de aplicación no seguro es una gran causa de vulnerabilidades en un sistema. La externalización del

desarrollo de un componente para ser utilizado por sus aplicaciones podría hacer que sean inseguras si la empresa subcontratada no sigue prácticas de codificación seguras.

- Almacenamiento de datos Es posible que esté almacenando datos con una empresa externa, tal vez como un sitio alternativo para almacenar copias de seguridad **de datos**. Verifique que la compañía de terceros esté protegiendo el sistema que contiene sus datos, pero también tome medidas propias para garantizar que los datos estén cifrados y que solo su empresa pueda descifrarlos.

Administración de parches inadecuada o débil

La falta de una estrategia de parches es una de las principales razones de los sistemas vulnerables porque un parche tiene las correcciones de seguridad para vulnerabilidades conocidas. Asegúrese de aplicar parches a lo siguiente regularmente:

- **Firmware** Aplique actualizaciones al firmware en dispositivos como servidores, enrutadores, conmutadores y cualquier otro dispositivo de hardware que pueda existir dentro de su empresa.

- **Sistema operativo (SO)** Parche el sistema operativo regularmente y busque software de administración de parches para automatizar la implementación de parches.

- **Aplicaciones** Asegúrese de que las aplicaciones también estén parcheadas. Una vulnerabilidad en una aplicación puede hacer que todo el sistema sea vulnerable a un ataque.

Plataformas heredadas

Los sistemas heredados son algo que debe tener en cuenta en la red, ya que muchos sistemas heredados ya no tienen soporte de proveedores, lo que significa que lo más probable es que ya no estén parcheados.

Además, un sistema heredado puede estar utilizando protocolos más antiguos que no son seguros. Si está utilizando sistemas heredados en su red, busque colocarlos en su propio segmento de red para ayudar a reducir las posibilidades de que los sistemas sean atacados.

Comprender el impacto de las vulnerabilidades

Una empresa que no aprenda a gestionar las vulnerabilidades que existen en un sistema podría enfrentarse a resultados desastrosos. Los siguientes son impactos potenciales para un negocio que no reduce las vulnerabilidades que existen en sus productos:

- **Pérdida** de datos Una vulnerabilidad en el sistema puede hacer que pierda el acceso a los datos. Por ejemplo, un atacante podría aprovechar la vulnerabilidad y eliminar los datos o cifrarlos con ransomware.

- **Violaciones** de datos Una violación de datos ocurre cuando una persona no autorizada obtiene acceso a datos confidenciales. Una violación de datos también se conoce como *fuga* de datos o *derrame de datos.* La violación de datos puede incluir información como registros de salud, datos financieros y propiedad intelectual. El impacto de una violación de datos podría ser desastroso para una empresa debido al costo de investigar y recuperarse de la violación de datos, pero la empresa también podría ver daños a su reputación.

- **Exfiltración de datos La exfiltración** de datos ocurre cuando alguien transfiere datos desde una computadora o red sin permiso para hacerlo. Ejemplos de datos confidenciales que un atacante puede querer transferir desde un sistema son datos financieros (como números de tarjetas de crédito), información de identificación personal (PII) y nombres de usuario y contraseñas. Para evitar la filtración de datos, puede deshabilitar los puertos USB para que el almacenamiento portátil, como unidades flash USB y unidades externas USB, no se pueda conectar a un sistema, o puede usar las características de prevención de pérdida de datos (DLP)

para impedir que los datos confidenciales se copien o envíen por correo electrónico fuera de la organización.

- **Robo** de identidad Una vulnerabilidad en un sistema podría resultar en el robo de identidad, donde se roba información personal sobre una persona, permitiendo al atacante asumir la identidad de la víctima.

- **Pérdidas** financieras Una vulnerabilidad podría resultar en pérdidas financieras debido a muchas razones. En primer lugar, la vulnerabilidad puede permitir que el atacante bloquee los sistemas de producción, lo que resulta en pérdidas de ingresos, pero también existe el costo de recuperar los sistemas y el costo intangible del daño a la reputación.

- **Daño** a la reputación Como ya se ha mencionado varias veces, una vulnerabilidad explotada que resulte en un compromiso del sistema podría causar daños a la reputación de la empresa. Los clientes pueden optar por dejar de hacer negocios con su empresa si sienten que sus datos no están seguros.

- **Pérdida** de disponibilidad Una vulnerabilidad podría provocar la pérdida de disponibilidad de un sistema o servicio. Por ejemplo, una vulnerabilidad en una base de datos back-end puede hacer que una aplicación web de comercio electrónico no pueda mostrar productos o tomar pedidos en línea.

Para el examen, recuerde que la exfiltración de datos es transferir datos de una computadora sin permiso y que puede reducir el riesgo de exfiltración de datos deshabilitando el uso de unidades USB e implementando soluciones de prevención de pérdida de datos (DLP).

Problemas de seguridad comunes y salida del dispositivo

Los sistemas y las redes pueden verse comprometidos de muchas maneras diferentes, pero la buena noticia es que la mayoría de los exploits y ataques se dirigen a un puñado de problemas de seguridad que podemos identificar y abordar. En esta sección aprenderá acerca de las estrategias para solucionar problemas de seguridad comunes y resultados comunes con diferentes tecnologías de seguridad. También aprenderá sobre los marcos de seguridad comunes y las guías que las organizaciones utilizan para desarrollar sus estrategias de seguridad.

Solución de problemas de seguridad comunes

El examen de certificación Security+ espera que conozca las razones comunes por las que ocurren incidentes de seguridad, como un pirata informático que explota un sistema, un usuario que elimina accidental o intencionalmente un archivo, o incluso un usuario que envía por correo electrónico datos confidenciales a alguien fuera de la empresa.

Configuración débil o configuración incorrecta Se producen varios incidentes de seguridad debido a problemas de configuración incorrecta o configuración de seguridad débil. Por ejemplo, una pequeña empresa puede configurar una red inalámbrica utilizando un enrutador inalámbrico y no cambiar ninguno de los valores predeterminados.

Las siguientes son configuraciones erróneas comunes de sistemas o dispositivos que causan problemas de seguridad:

■ Credenciales sin cifrar/**texto sin cifrar** Muchas tecnologías y protocolos de Internet no cifran el tráfico de red de forma predeterminada, incluidos el nombre de usuario y la contraseña utilizados para iniciar sesión en el dispositivo. Asegúrese de utilizar tecnologías de cifrado como SSL/TLS, VPN y versiones seguras de protocolos cuando sea posible.

■ **Registros y anomalías de** eventos Cuando mire sus registros de eventos y registros de actividad, asegúrese de estar atento a los eventos anormales que aparecen en el registro. Cualquier actividad sospechosa debe investigarse más a fondo. Desde el punto de vista de una configuración incor-

recta, compruebe que el registro está habilitado y que sabe dónde se almacenan los registros para el sistema y los dispositivos.

- **Problemas de** permisos No configurar los permisos adecuados en los recursos es una razón común por la que los ataques internos son tan exitosos. Asegúrese de revisar los permisos de recursos de forma regular y solo otorgue los permisos necesarios (principio de privilegios mínimos).

- **Violaciones** de acceso Una violación de acceso ocurre cuando alguien que no está autorizado para acceder a un sistema obtiene acceso. Asegúrese de requerir autenticación antes de que alguien pueda obtener acceso a una red o sistema, y asegúrese de que el tráfico de inicio de sesión esté cifrado. Configure permisos en los recursos para asegurarse de que nadie pueda obtener acceso a un recurso que no deba tener acceso.

- **Emisión de** certificados Los certificados son archivos electrónicos que contienen claves utilizadas para cifrar la comunicación. Los certificados deben usarse para proteger el tráfico web, el tráfico de correo electrónico y la comunicación de servidor a servidor, como mínimo. Asegúrese de que los certificados que se usan no han caducado, no se han revocado y provienen de una entidad de certificación (CA) de confianza. Aprenderá más sobre los certificados en **los capítulos 12** y **13**.

- **Exfiltración** de datos Como se mencionó anteriormente, la exfiltración de datos ocurre cuando alguien transfiere información de un sistema sin permiso. Recuerde para el examen que para evitar la exfiltración de datos, puede deshabilitar los puertos USB o puede usar las funciones DLP para bloquear la copia de datos confidenciales o el correo electrónico fuera de la organización.

- **Dispositivos mal configurados** La mala configuración del dispositivo es una gran razón por la que los atacantes pueden obtener acceso a sistemas a los que no deberían poder acceder. Asegúrese de configurar lo siguiente:

■ **Cortafuegos** Asegúrese de que los cortafuegos se utilizan para dividir la red en diferentes segmentos de red. Un firewall con reglas mal configuradas permite a los usuarios acceder a segmentos de red a los que no deberían tener acceso. Asegúrese de que el firewall de cada segmento de red esté configurado correctamente para controlar qué tráfico puede pasar a través del firewall para llegar a ese segmento de red específico.

■ **Filtro** de contenido Los dispositivos de filtrado de contenido se utilizan para controlar a qué contenido de Internet pueden acceder los empleados. Si las reglas de filtrado de contenido no están configuradas correctamente, los usuarios podrían estar visitando sitios no seguros y tener código ejecutado en sus sistemas.

■ **Puntos de acceso** Los puntos de acceso inalámbricos y los routers domésticos inalámbricos suelen estar mal configurados. Asegúrese de revisar la configuración de sus puntos de acceso inalámbricos y asegúrese de que ha configurado características como el filtrado MAC, el cifrado WPA2 y una clave de cifrado segura y que ha modificado la contraseña de administrador predeterminada.

■ Configuraciones de seguridad débiles Una gran razón para los incidentes de seguridad es la configuración **de seguridad** débil. Por ejemplo, un administrador de red puede configurar el cifrado en la red inalámbrica, pero elegir un método de cifrado más débil o tal vez utilizar una clave de cifrado débil. Asegúrese de revisar todas las configuraciones de seguridad en los dispositivos, como listas de control de acceso, contraseñas, claves de cifrado, algoritmos de cifrado y cualquier función de filtrado que pueda estar disponible.

Cuestiones de personal Puede configurar los mejores ajustes de seguridad en sus dispositivos y aún pueden ser fáciles de piratear si no se enfoca en capacitar a los empleados para que sean conscientes de la seguridad. También debe estar atento a las amenazas internas. Las siguientes

son consideraciones de seguridad clave que implican problemas de personal:

- **Violación de la política** Muchos incidentes de seguridad ocurren porque los empleados violan las políticas de seguridad de la empresa. Asegúrese de educar a los empleados sobre las políticas de seguridad y por qué están vigentes. Es menos probable que los empleados violen las políticas de seguridad si entienden por qué existen las políticas y cómo el cumplimiento de ellas protege a la empresa y sus activos.

- **Amenaza interna** La mayoría de las empresas se centran en los cortafuegos como su protección de seguridad. Eso es importante, por supuesto, pero también debe proteger los activos de la empresa de amenazas internas, como empleados descontentos. Asegúrese de usar autenticación, permisos y listas de control de acceso para controlar a qué tienen acceso los empleados. También asegúrese de implementar software antimalware para proteger sus sistemas internos de virus.

- Ingeniería social Educar a los empleados sobre los ataques comunes de ingeniería social para que puedan identificar cuándo están siendo blanco de la ingeniería **social**. La educación es la clave para protegerse contra los ataques de ingeniería social.

- **Redes** sociales Educar a los empleados sobre qué información puede y no puede publicarse en las redes sociales. Debe tener políticas estrictas que restrinjan las fotos del lugar de trabajo que se publican en las redes sociales porque pueden contener información confidencial. Por ejemplo, una imagen de un empleado sentado en su escritorio también puede mostrar un documento confidencial abierto en la pantalla en el fondo o un documento en el escritorio.

- **Correo** electrónico personal Muchos empleados utilizan su cuenta de correo electrónico personal en el trabajo y podrían utilizarla para enviar por correo electrónico datos de la empresa fuera de la empresa.

Asegúrese de tener características DLP para protegerse contra fugas de datos. También tenga en cuenta el almacenamiento personal en la nube que los empleados pueden usar para transferir datos hacia y desde el trabajo. Puede considerar bloquear el acceso a estos sitios en el firewall o dispositivo de filtrado de contenido.

Problemas de aplicación

El software es otra área de preocupación con la seguridad. Debe tener en cuenta todas las siguientes cuestiones relacionadas con las aplicaciones:

- **Software no autorizado** Las organizaciones deben tener políticas estrictas en cuanto a qué software se permite o no se puede ejecutar en los sistemas de la empresa. *La lista blanca de aplicaciones* se refiere a definir qué software puede ejecutarse en un sistema. Puede usar una herramienta como Windows AppLocker como parte de la directiva para restringir qué software puede ejecutarse en un sistema.

- Desviación de línea base Una **línea base de** seguridad es un estado de seguridad definido del que los sistemas no deben desviarse. Cualquier modificación de un sistema que pueda abrir el sistema y hacerlo menos seguro debe ser examinada primero y monitoreada de cerca si se implementa. Las organizaciones pueden usar tecnologías como la Configuración de estado deseado (DSC) de PowerShell para evitar cambios en un sistema que se desvíen de la línea base.

- **Violación del cumplimiento de la licencia (disponibilidad/integridad)** Las empresas pueden enfrentar multas graves si se descubre que no cumplen con las licencias de software. Hay herramientas disponibles que le permiten realizar un seguimiento de la instalación del software y garantizar que no exceda el número de instalaciones con licencia permitidas.

- **Gestión de activos** Una vez que un sistema se pone en producción, debe mantener ese sistema para mantenerlo seguro. Mantener los sistemas de

forma centralizada es la clave del éxito con la gestión de activos. Use productos como objetos de directiva de grupo (GPO) y Microsoft Endpoint Configuration Manager (MECM) para administrar la implementación de configuraciones, revisiones, controladores y aplicaciones.

- **Problemas de** autenticación Asegúrese de que las aplicaciones estén configuradas para la autenticación de la manera más segura para que alguien no pueda aprovechar el tráfico de autenticación y obtener acceso a la red utilizando las credenciales utilizadas por la aplicación. Asegúrese de que las aplicaciones utilizan sus propias cuentas y no cuentas predeterminadas, como la cuenta del sistema o la cuenta "sa" al conectarse a una base de datos.

Análisis e interpretación de resultados de tecnologías de seguridad

Hay una serie de diferentes dispositivos y tecnologías de seguridad que muestran mensajes a los usuarios o proporcionan información a los administradores de sistemas para que estén al tanto de los posibles incidentes de seguridad que se producen. En la lista siguiente se identifican los resultados que vería de estas tecnologías de seguridad:

- HIDS/HIPS Un sistema de detección de intrusiones basado en host (HIDS) o un sistema de prevención de intrusiones basado en host (**HIPS**) muestra notificaciones de amenazas potenciales dentro de la aplicación o las envía a una dirección de correo electrónico designada. Revise los eventos de notificación para identificar cualquier actividad sospechosa en el sistema. Al mirar la salida, revise la fecha y hora del evento, el origen del evento (la mayoría de los productos HIDS/HIPS revisan los registros de muchas fuentes) y la cuenta que causó el evento. Con esta información, puede decidir si es necesario realizar un cambio de configuración.

- **Antivirus** El software antivirus proporciona registros y notificaciones. Revise estos registros y notificaciones para obtener información como el resultado de un análisis programado, que informará si se encontró malware y, de ser así, el nombre del malware y los nombres de los archivos

infectados. También recibirá información sobre cualquier acción correctiva tomada, como si un archivo infectado se eliminó del sistema o se movió a un área de cuarentena.

■ **Comprobación** de integridad del archivo Cuando ejecute herramientas que comprueben la integridad del archivo, le informarán si ha habido cambios en el archivo desde que se calculó el valor hash del archivo. Puede recibir resultados de comprobaciones de integridad de archivos, como "discrepancia de hash" o "discrepancia de firma", lo que significa que el archivo se ha alterado. Los resultados como "hash match", "hash valid" o "signature verified" le permiten saber que el archivo no ha cambiado.

■ **Firewall basado** en host Los firewalls basados en host generalmente escriben en los registros o muestran alertas si interrumpen el tráfico debido a reglas configuradas en el sistema. Busque la salida que contenga información como "paquete descartado src = 24.35.45.3: 63378 TCP dst = 32.46.58.62: 80 TCP". Dentro de esta información, debería ver las direcciones IP de origen y destino (24.35.45.3 y 32.46.58.62), los números de puerto utilizados por los sistemas de origen y destino (:63378 y :80) y el protocolo (TCP).

■ **Lista** blanca de aplicaciones La lista blanca de aplicaciones es configurar un sistema para una lista de software aprobado que se puede utilizar en el sistema. Si alguien intenta instalar o ejecutar una aplicación que no está en la lista, recibirá un mensaje de error que indica que la aplicación no está autorizada. Puede usar AppLocker en Windows para crear una lista de aplicaciones autorizadas para ejecutarse en el sistema.

■ Control de medios extraíbles El control de medios extraíbles es cuando se controla a qué medios se puede acceder en un sistema, como unidades de disco óptico y **medios extraíbles** (por ejemplo, unidades USB externas). Cuando los usuarios intentan conectarse o acceder a una unidad que no se les permite usar, normalmente ven aparecer una notificación en la

pantalla que indica que no están autorizados para acceder a la unidad. Puede configurar el control de medios extraíbles a través de directivas de grupo en Windows, como se muestra en el próximo **ejercicio 5-1**.

- **Herramientas avanzadas de malware** Las herramientas avanzadas de malware le notifican el malware que se detectó y proporcionan información detallada sobre el malware. También informan si el malware se eliminó con éxito o se movió a un área de cuarentena.

- **Herramientas** de gestión de parches Las herramientas de gestión de parches están diseñadas para ayudar en el despliegue de parches en los sistemas de la red. Con las herramientas de administración de revisiones, debería ver resultados, como qué parches requiere un sistema y actualizaciones de estado cuando implementa un parche en un sistema. Si por alguna razón no se aplicó un parche a uno o más sistemas, también se le notificará.

- UTM Un sistema *unificado de gestión de amenazas (UTM)* es un dispositivo que combina una serie de funciones de seguridad, como un firewall, IDS / IPS, antivirus de puerta de enlace y antispam de puerta de enlace, filtrado de contenido y prevención de pérdida de datos, por nombrar algunas tecnologías de seguridad integradas. Los sistemas UTM generan una serie de información, como alertas de tráfico sospechoso, informes sobre el número de virus y mensajes de spam bloqueados, y resúmenes del número de infracciones de filtro de contenido.

- Las soluciones de prevención de pérdida de datos (DLP) **DLP** evitan que los usuarios puedan enviar información confidencial fuera de la empresa. Cuando un usuario intenta copiar datos en una unidad USB, puede recibir un mensaje de error de la solución DLP que indica que no tiene permisos, o si un usuario intenta enviar un correo electrónico que contiene información confidencial bloqueada por DLP, el usuario normalmente recibirá un correo electrónico que indica que el contenido no se envió debido a una infracción de DLP.

■ **Prevención** de ejecución de datos La prevención de ejecución de datos (DEP) es una función que se puede habilitar para evitar que el código de la aplicación se ejecute en áreas de memoria utilizadas para almacenar datos (conocidas como páginas de datos). Con DEP, los bloques de memoria no utilizados para ejecutar un programa son marcados como páginas no ejecutables por el sistema para que el software malintencionado no se ejecute en ese bloque de memoria. Puede verificar que DEP esté habilitado en su sistema yendo a un símbolo del sistema y escribiendo **wmic OS Get DataExecutionPrevention_SupportPolicy**. Recibirá una salida de 0 (siempre desactivada), 1 (siempre activada), 2 (activada para archivos binarios de Windows) o 3 (activada para todos los programas y servicios).

■ **Firewall** de aplicaciones web Un firewall de aplicaciones web está diseñado para proteger los servidores web del tráfico malicioso y solo permitir que el tráfico a la aplicación web pase a través del firewall. El tráfico bloqueado por el firewall se escribe en un archivo de registro para que el administrador de sistemas pueda revisar el tráfico bloqueado.

EJERCICIO 5-1

Control de medios extraíbles

En este ejercicio, deshabilite el acceso de escritura a medios extraíbles a través de directivas en el sistema y, a continuación, intente guardar un archivo en una unidad extraíble para revisar la salida proporcionada por el sistema.

1. Inicie sesión en la máquina virtual de Windows 10 y luego haga clic en el botón Inicio.

2. Escriba **gpedit.msc** y presione enter para iniciar el Editor de políticas de grupo local.

3. Expanda Configuración del equipo | Plantillas administrativas | Sistema y, a continuación, seleccione Acceso al almacenamiento extraíble.

4. Aquí verá una serie de políticas para deshabilitar el acceso de ejecución, lectura o escritura a diferentes tipos de medios. Haga doble clic en la directiva Discos extraíbles: Denegar acceso de escritura y, a continuación, elija Habilitar.

5. Haga clic en Aceptar para cerrar la pantalla de directivas y haga clic en el botón × para cerrar la ventana Editor de directivas de grupo local.

6. Inserte una unidad USB en el sistema e intente crear un archivo en la unidad USB.

   ¿Tuviste éxito? _____

   ¿Qué mensaje recibiste? _____

7. Cierre todas las ventanas.

Vulnerabilidades basadas en la nube frente a vulnerabilidades locales

Las vulnerabilidades contenidas en este capítulo en su mayor parte se analizaron teniendo en cuenta las redes locales, lo que significa que estas son vulnerabilidades que encontraría en sistemas y dispositivos dentro de su LAN.

También podrían existir varias vulnerabilidades comunes en entornos de nube, y la mayoría de ellas se ocupan de errores de configuración:

■ **Puertos abiertos** Asegúrese de no abrir puertos innecesarios en recursos de la nube, como máquinas virtuales (VM) o aplicaciones. Por ejemplo, muchos administradores de TI crearán una máquina virtual de Azure y, a continuación, abrirán el puerto de Protocolo de escritorio remoto (RDP) para acceder de forma remota a la máquina virtual. En este caso, Azure tiene una opción de host bastión disponible para que no sea necesario abrir el puerto RDP en cada una de las máquinas virtuales.

■ **Métodos** de autenticación Debido a que se puede acceder a las aplicaciones en la nube desde cualquier parte del mundo, debe configurar la autenticación multifactor (MFA) para que si usted u otra persona intenta iniciar sesión con su cuenta, se envíe un código de autenticación a su teléfono que debe ingresarse para que se produzca la autenticación.

■ **Políticas de** acceso condicional Puede utilizar directivas de acceso condicional para ayudar a mejorar la seguridad y proteger los recursos contra contraseñas débiles o autenticación débil. Las directivas de acceso condicional le permiten establecer restricciones para los usuarios al acceder a los recursos en la nube. Por ejemplo, puede hacer que las directivas se apliquen a usuarios, grupos, dispositivos e incluso a su ubicación IP.

■ Demasiados privilegios Esté atento a los usuarios que reciben **demasiados privilegios** dentro del entorno de nube (por ejemplo, agregar usuarios innecesarios al grupo Administradores globales).

OBJETIVO DE CERTIFICACIÓN 5.02

Identificación de amenazas físicas

Antes de sumergirme en los diferentes tipos de software malicioso, quiero familiarizarlo con algunas de las amenazas físicas populares que experimentan las empresas en el mundo real. En esta sección, discuto algunos tipos comunes de amenazas físicas a sistemas y dispositivos y

también discuto cómo minimizar las amenazas contra los activos de su empresa.

Husmeando

En el **capítulo 4** se le presentó el concepto de buceo en contenedores de basura, que implica que el hacker revise su basura y tome documentos confidenciales que podrían ayudar con un ataque. Un contenedor de basura hacker no solo podría sumergirse en su negocio, sino que sus empleados también podrían husmear en los papeles en el escritorio de otra persona o incluso revisar su archivador mirando documentos que no son de su incumbencia.

Para proteger la información de tales ataques de espionaje, asegúrese de implementar una política de escritorio limpio dentro de la empresa. Una Un especifica que los documentos confidenciales no deben dejarse a la intemperie y deben archivarse cuando no estén en uso.

También debe proteger la información que se coloca en los archivadores asegurándose de que los archivadores estén en un área segura y bloqueados para evitar que personas no autorizadas accedan a la información.

Debe saber que todos los documentos deben triturarse antes de desecharse para protegerlos del espionaje o el buceo en contenedores de basura.

Eduque a todos los empleados en el negocio para asegurarse de que trituren todos los documentos para ser desechados y no tiren documentos sin triturar directamente a la basura o papelera de reciclaje. ¡Todos los documentos de la compañía que se eliminan deben hacer un viaje a través de la trituradora primero!

Robo y pérdida de activos

Muchas amenazas de seguridad física son planteadas por equipos perdidos o robados, como una computadora portátil o un dispositivo móvil (teléfono inteligente, tableta, etc.). Muchas empresas tienen una política de que si un empleado deja una computadora portátil o dispositivo móvil de la empresa en un automóvil, no debe dejarlo a la vista, para evitar el robo de aplastar y agarrar. En este caso, algunas empresas especifican en la política que el empleado es responsable del reemplazo de la computadora portátil o dispositivo electrónico. Se recomienda a los empleados que coloquen todos los dispositivos electrónicos bloqueados en el maletero de su automóvil en lugar de dejarlos visibles en el asiento del pasajero o en el asiento trasero del automóvil. Cabe señalar que algunas organizaciones pueden reprender a los empleados por no seguir dichas políticas para garantizar que los empleados vean el valor de tomar decisiones responsables con los activos de la empresa.

Dentro de la oficina, puede ayudar a disuadir el robo de equipos como computadoras portátiles, monitores de pantalla plana, proyectores e incluso computadoras de escritorio mediante el uso de un cable de bloqueo. Un *cable de bloqueo* es un cable pequeño que está conectado y bloqueado al dispositivo y que asegura el dispositivo al escritorio. Estos cables de bloqueo no van a evitar que un ladrón determinado robe el equipo, sino que actuarán como un elemento disuasorio y evitarán que alguien pase casualmente y pase el equipo. **La figura 5-1** muestra un cable de bloqueo.

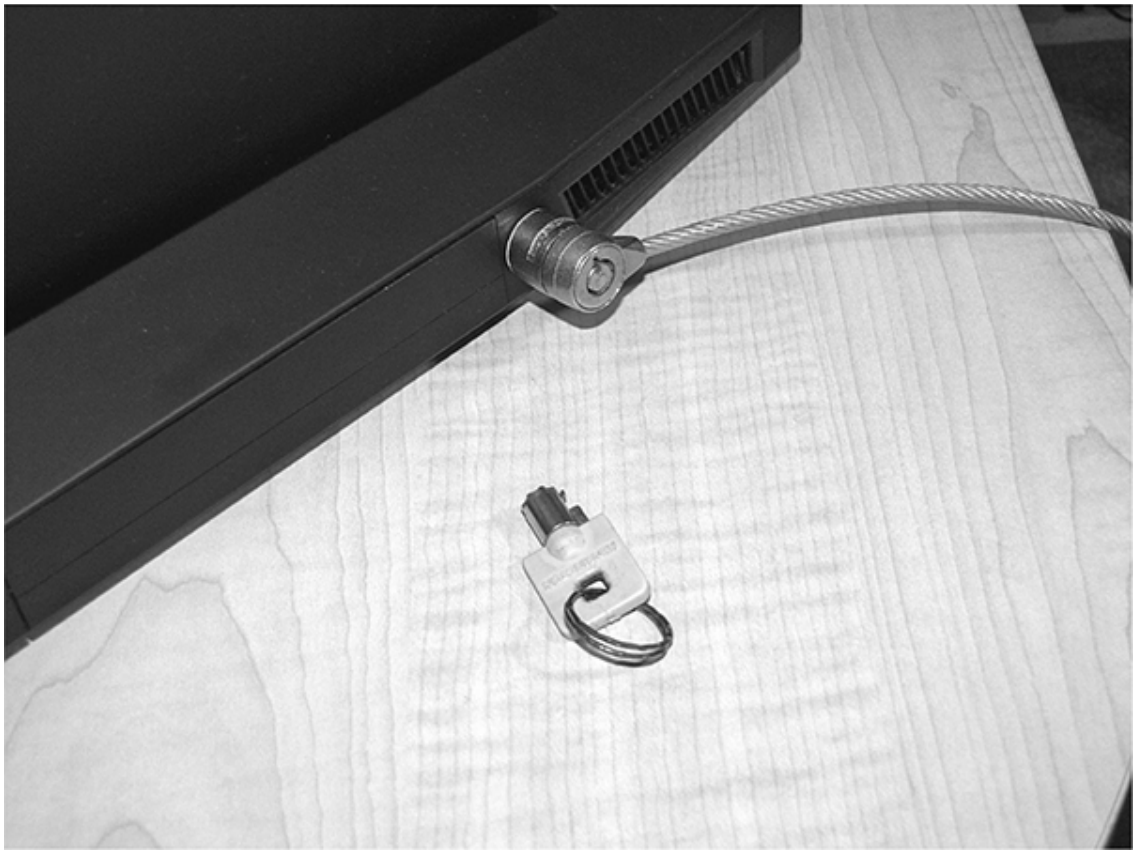


FIGURA 5-1

Uso de un cable de bloqueo para ayudar en la seguridad física

Borrado remoto del dispositivo

Asegúrese de que los empleados sepan la importancia de informar inmediatamente sobre dispositivos móviles perdidos o robados para que pueda borrar estos dispositivos de forma remota lo más rápido posible. Borrar un dispositivo envía una señal desde el servidor al dispositivo para borrar todos sus datos y su configuración. Esto garantiza que un dispositivo móvil perdido o robado no tenga información confidencial.

Protecciones en el dispositivo

Es importante que implemente salvaguardas en su equipo móvil para que, si es robado o perdido, haga que sea lo más difícil posible para alguien usar el dispositivo.

La mayoría de los dispositivos admiten la configuración de algún tipo de contraseña o código PIN para que si alguien roba el dispositivo, necesiten saber el código de acceso para usarlo. La mayoría de los dispositivos móviles, como iPhones y Androids, admiten el bloqueo del dispositivo después de un cierto período de no uso (conocido como bloqueo automático). Esta función de bloqueo significa que si el dispositivo se pierde o es robado, alguien que encuentre o robe el dispositivo necesitará saber el código de desbloqueo para acceder a él. También es posible que desee habilitar cualquier función de seguimiento de dispositivos que el dispositivo pueda admitir para que pueda localizar el dispositivo en caso de pérdida o robo.

Cuando se trata de computadoras portátiles, asegúrese de establecer una contraseña de encendido del BIOS en el dispositivo y también de cambiar el orden de arranque en la computadora portátil para que alguien no pueda arrancar desde CD-ROM e instalar su propio sistema operativo si roba el dispositivo. Asegúrese de establecer la contraseña de administrador del BIOS para que alguien no pueda entrar en el BIOS y realizar cambios, como alterar el orden de arranque.

Si no puede establecer una contraseña de arranque en el BIOS, considere el cifrado completo de la unidad con una herramienta como BitLocker, que es una característica de cifrado de unidad integrada en los sistemas Windows que no solo cifra el contenido de la unidad, sino que también actúa como una contraseña de arranque.

Cifrado de datos

En el **Capítulo 12** aprenderá sobre el cifrado, pero es importante tener en cuenta aquí que un gran paso para proteger sus datos confidenciales en una computadora portátil o dispositivo móvil es cifrar esos datos en caso de que el dispositivo se pierda o sea robado. Si los datos están encriptados, entonces ha garantizado la seguridad de los datos de la empresa, incluso si su dispositivo se ha perdido o ha sido robado. Una vez más, un buen ejemplo de una tecnología que podría usarse para cifrar todo el disco es BitLocker.

Al planificar la seguridad de los dispositivos móviles, siempre asuma que el dispositivo caerá en manos de una parte que no sea de confianza. Por lo tanto, debe asegurarse de utilizar funciones como el bloqueo automático y el cifrado de datos en el dispositivo para mantener la confidencialidad de sus datos.

Fallo humano

Otra amenaza importante de seguridad física contra los sistemas que debe tener en cuenta es el error humano. Por ejemplo, un empleado que intenta realizar una actualización de un sistema, tal vez agregando memoria o reemplazando un disco duro, podría freír la placa base del sistema a través de *una descarga electrostática (ESD).* ESD es la acumulación de electricidad estática en usted mismo que se transfiere a otro objeto, como un componente de la computadora, cuando lo toca. Esta transferencia de electricidad estática es suficiente para matar o dañar seriamente los componentes de la computadora.

Para evitar este tipo de situaciones, eduque al equipo de soporte de escritorio sobre ESD y sobre el uso de una correa de muñeca antiestática para conectarse siempre a tierra antes de reparar los sistemas.

Sabotaje

Otra amenaza común contra los sistemas es el sabotaje, que es típicamente, pero no siempre, el resultado de un empleado descontento. Es importante identificar situaciones en las que los activos de la empresa son vulnerables al sabotaje. Demasiadas veces en mis cursos de seguridad escucho historias de estudiantes sobre incidentes en los que una base de datos de la empresa fue manipulada por un empleado descontento.

Debe identificar los sistemas que son susceptibles de sabotaje y asegurarse de tener un plan de recuperación para esos sistemas. Un *plan de recuperación* implica procedimientos paso a paso para recuperar el sistema, pero también garantiza que tenga piezas de repuesto adecuadas en el estante de la sala de servidores.

OBJETIVO DE CERTIFICACIÓN 5.03

Mirando el software malicioso

Ahora que comprende algunas de las amenazas físicas populares contra los sistemas, echemos un vistazo a algunos tipos de software malicioso que representan una amenaza para los sistemas actuales. El software malicioso es cualquier software que daña o hace un mal uso del sistema, lo que incluye eliminar archivos del sistema, monitorear la actividad en el sistema e incluso algo tan simple como ralentizar el sistema.

Escalada de privilegios

La escalada de privilegios es cuando un hacker encuentra una falla en el sistema operativo, o en una pieza de software instalada en el sistema, que, cuando se explota, eleva los privilegios del hacker de las capacidades normales del usuario al acceso administrativo. Una vez que el hacker ha obtenido acceso administrativo al sistema, puede realizar los cambios que desee en el sistema, incluida la colocación de una puerta trasera para el acceso futuro.

Hay tres tipos de escalada de privilegios:

- **Escalada vertical** de privilegios Cuando alguien con acceso de usuario normal puede elevar sus privilegios a acceso administrativo

- **Escalada horizontal de privilegios** Cuando se mantiene el mismo nivel de acceso, pero el recurso al que se accede es diferente

- Reducción de privilegios Cuando alguien con acceso administrativo puede reducir su nivel **de privilegios** para que pueda acceder a los datos a los que un usuario específico tiene acceso

Virus

Una de las mayores áreas de preocupación con la seguridad es cuando un sistema es superado por un virus. Un virus es un software malicioso que infecta un sistema como una computadora, tableta o teléfono inteligente. La infección puede destruir datos en el sistema, evitar que el sistema arranque o simplemente usar recursos en el sistema, lo que resulta en ralentizar el sistema. En esta sección se describen los tipos comunes de virus.

Virus ejecutable

Los virus más antiguos eran virus ejecutables, donde el virus se adjuntaba a un archivo ejecutable pero no se activaba hasta que se ejecutaba el archivo. Este virus se propagaba típicamente de un sistema a otro por el usuario compartiendo archivos a través de disquetes, unidades flash o una unidad de red.

Virus del sector de arranque

Un virus del sector de arranque es un virus grave que ataca el código del sector de arranque y lo sobrescribe. El sector de arranque es el primer sector del disco y contiene el código del cargador del sistema operativo que inicia la secuencia de arranque. Cuando un virus del sector de arranque sobrescribe este sector, impide que el sistema arranque desde el disco infectado.

Macro Virus

La mayoría de las aplicaciones actuales admiten macros, que son una forma de automatizar una tarea dentro de la aplicación de software. Con la suite Microsoft Office, por ejemplo, podemos crear macros usando Visual Basic para Aplicaciones (VBA), que es un poderoso lenguaje de programación que puede manipular la aplicación y el sistema operativo.

Un virus de macro es un código escrito con un lenguaje de macros que realiza una acción maliciosa, como eliminar archivos o enviar correos electrónicos a todos los usuarios de la libreta de direcciones. La macro

generalmente se crea en un archivo y luego se desencadena automáticamente cuando alguien abre el archivo.

Virus de la bomba lógica

Una bomba lógica es un tipo de virus que se planta en el sistema mediante la instalación de una pieza de software que contiene la bomba lógica. La aplicación de software que instaló actúa como se supone que debe hacerlo hasta que se produce un determinado evento, como una fecha específica. Cuando ejecuta el software, siempre comprueba esa fecha específica y, si el software se ejecuta en esa fecha, realiza su acto malicioso. Este es un método común que los empleados descontentos han utilizado para sabotear los datos de la empresa después de renunciar o ser despedidos. Programan el software (que normalmente funciona bien) para eliminar datos en una fecha específica.

Para el examen, sepa que el virus de la bomba lógica espera a que ocurra un evento específico, como una fecha determinada, antes de activarse.

Virus gusano

Un virus gusano es un virus dañino y común hoy en día. El virus gusano es un tipo de virus aterrador porque tiene la característica única de poder replicarse sin necesidad de que un usuario lo active. Los virus de gusano pueden replicarse de varias maneras:

- **Protocolos** de red Un virus gusano puede replicarse automáticamente a través de la red mediante el uso de protocolos de red estándar y comprometer un sistema a través de vulnerabilidades en las aplicaciones de red que se ejecutan en el sistema. Un buen ejemplo es el gusano Blaster de 2003 que se replicaba a través del puerto RPC (puerto 135). ¿Quién podría olvidar el virus del gusano SQL Slammer, también de 2003, que infectó aproximadamente 75.000 sistemas en Internet en 10 minutos? SQL

Slammer aprovechó una vulnerabilidad conocida de desbordamiento de búfer en SQL Server y se conectó a servidores SQL Server sin revisión a través del puerto UDP 1434.

- **Los virus de gusanos de** correo electrónico se pueden propagar automáticamente mediante el correo electrónico. El virus se envía a un usuario en un mensaje de correo electrónico, y cuando ese usuario abre el mensaje, el código del virus se ejecuta y recorre la lista de contactos del usuario y envía el correo electrónico a todos los contactos. Ejemplos de virus de correo electrónico infames son el virus ILOVEYOU en 2000 y el virus que se envió con una línea de asunto que dice "Aquí tienes" en 2010.

- **Unidades** flash Una nueva ola de virus gusanos infecta los sistemas mediante la replicación mediante el uso de unidades flash (memorias USB). Una vez que el virus del gusano está en un sistema, espera a que alguien conecte una unidad flash en ese sistema, y el virus del gusano se replica en la memoria USB. El usuario lleva la memoria USB a otro sistema, y una vez que la unidad está conectada al puerto USB, el virus se replica desde la memoria USB al sistema. Conficker era un virus gusano que podía replicarse mediante el uso de memorias USB.

Virus troyano

Un virus troyano es un programa que un usuario es engañado para instalar porque parece hacer algo útil, pero en realidad, es un virus que infecta el sistema. El virus troyano normalmente modifica el sistema abriendo un puerto TCP / IP en el sistema, lo que permite al pirata informático conectarse al sistema y tomar el control de él.

Cabe señalar que el virus troyano puede hacer más que abrir un puerto en el sistema, y debido a que la mayoría de las personas tienen firewalls hoy en día para bloquear el acceso al puerto que abre el troyano, puede encontrar que el virus troyano pone adware en el sistema o un keylogger.

La Tabla 5-1 enumera los virus troyanos populares y los puertos que abren en un sistema.

TABLA 5-1

Números de puerto populares de virus troyanos

Protocol	Port	Trojan
TCP	12345	NetBus
TCP	17300	Kuang
TCP	27374	SubSeven
TCP	31337	BackOrifice
TCP	48006	FraggleRock

Debe saber que un virus troyano generalmente abre un puerto TCP / IP en el sistema para actuar como una puerta trasera para el pirata informático. También debe saber que un virus gusano es un virus autorreplicante.

Solución de problemas de virus troyanos

Antes de dejar el tema de los virus troyanos, quiero hablar sobre algunos comandos comunes de Windows que se pueden usar para rastrear un virus troyano si sospecha que ha sido infectado. El objetivo aquí es finalizar el programa que abrió el puerto para que el puerto se cierre.

El primer comando a utilizar para rastrear un virus troyano es el comando **netstat**. Si utiliza el comando **netstat -na**, verá una lista de puertos locales que están en estado de escucha. *Escuchar* significa que el puerto está abierto y esperando que alguien se conecte a él, en lugar de alguien que realmente está conectado en ese momento.

Para averiguar qué programa abrió el puerto, puede agregar el modificador **-o** a **netstat**, que muestra el número de ID de proceso (PID) del programa que abrió el puerto. En la **figura 5-2**, observe que el puerto 12345 (el puerto NetBus) está en estado de escucha y que el PID responsable de abrir el puerto 12345 es el número 208.

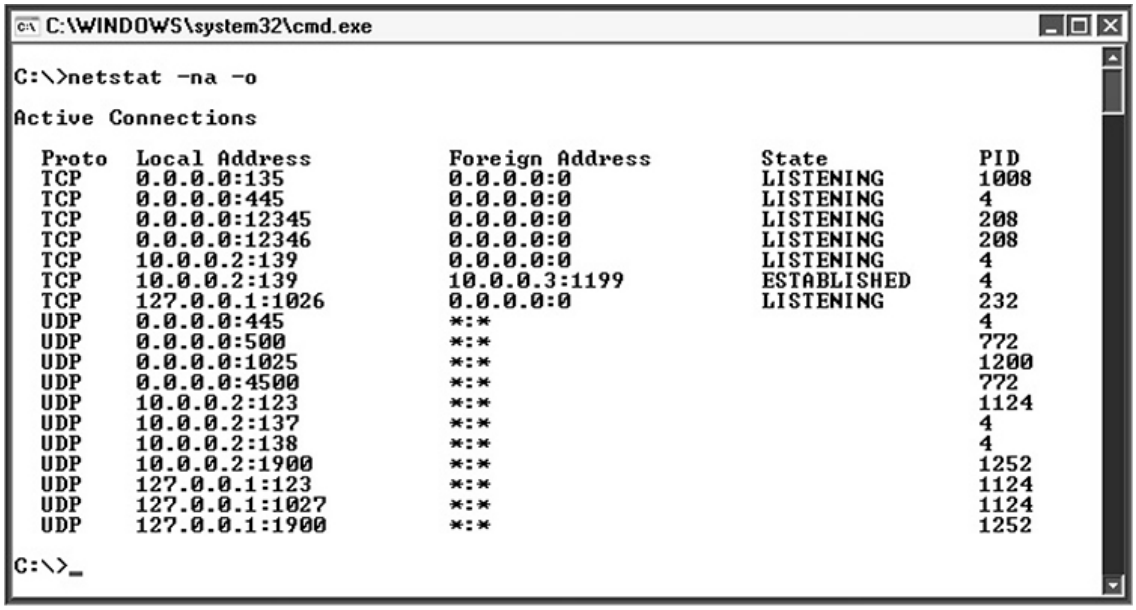


FIGURA 5-2

Uso de netstat para mostrar el ID de proceso del programa que abrió el puerto

Una vez que tenga el número de ID de proceso de la aplicación responsable de abrir el puerto, puede rastrear el archivo EXE asociado con ese ID de proceso. Si utiliza el comando **tasklist**, verá los procesos (archivos EXE) que se ejecutan en la memoria y el PID asociado con cada proceso (consulte la **figura 5-3**). Observe en la salida que sigue que el parche .exe es el archivo EXE asociado con el PID y es responsable de abrir el puerto. Tenga en cuenta también que puede utilizar la función de canalización (|) para buscar una entrada específica con el comando **tasklist**. Por ejemplo, puede usar tasklist | find "208" para buscar una entrada que contenga "**208"** en los resultados.

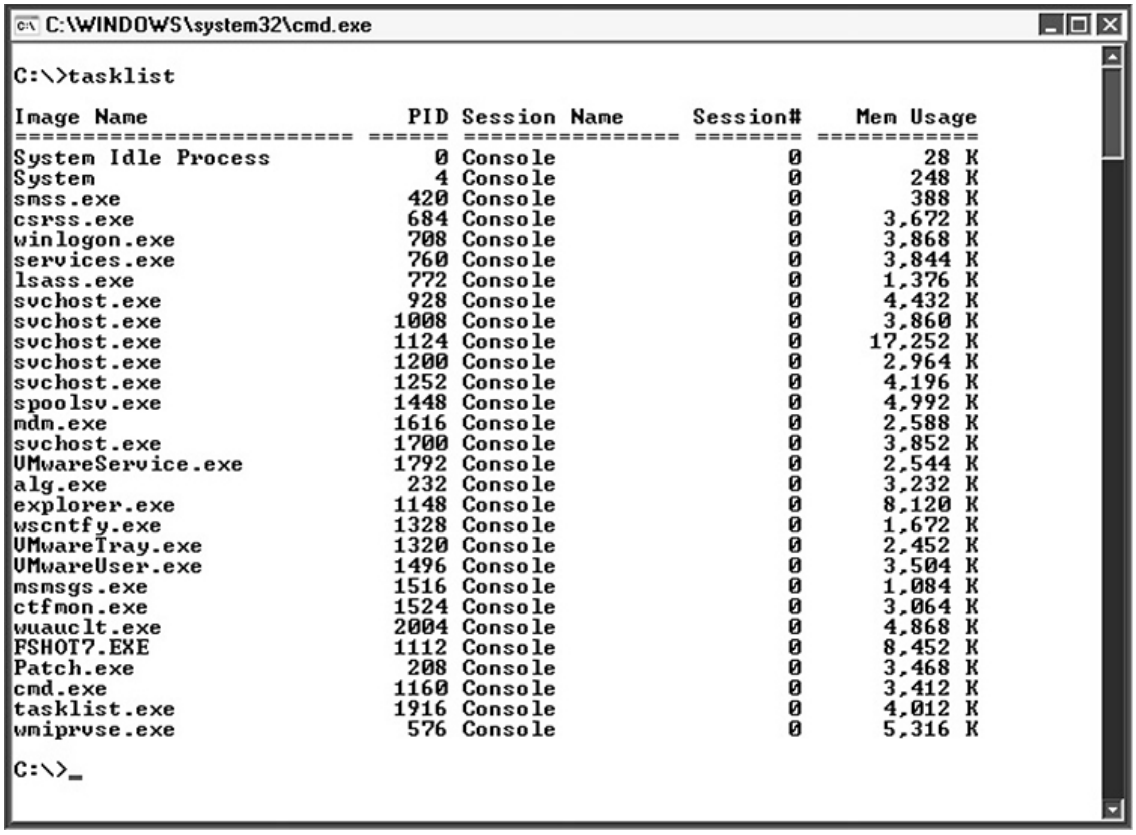


FIGURA 5-3

Uso de la lista de tareas para mostrar los ejecutables que se ejecutan en memoria

Una vez que haya utilizado el comando **tasklist** y conozca el proceso, puede matar el proceso con el comando **taskkill**. Con el comando **taskkill**, puede especificar el archivo EXE para matar o buscar el PID mediante el modificador /**PID**. El código que se muestra en la **figura 5-4** utiliza el comando **taskkill** para forzar la eliminación de un proceso por su número PID.

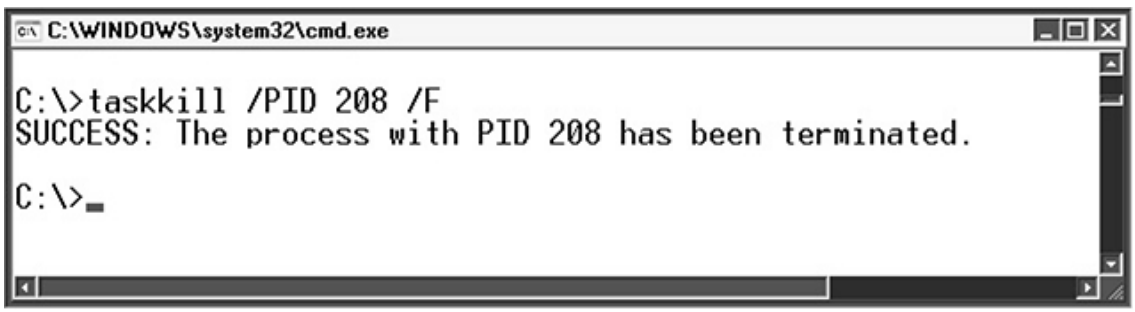


FIGURA 5-4

Uso de taskkill para terminar un programa que se ejecuta en memoria

Después de matar el proceso, asegúrese de verificar las áreas de configuración en el sistema que normalmente inician los programas automáticamente. Este sería el grupo de programas Inicio en el menú Inicio y también la parte Ejecutar del Registro en HKLM\Software\Microsoft\Windows\CurrentVersion\Run (consulte la **figura 5-5**). En nuestro ejemplo, si ejecuta regedit.exe y navega a la parte Ejecutar del registro, verá que el parche .exe está configurado para ejecutarse automáticamente cuando se reinicia Windows. Debe eliminar esta entrada.

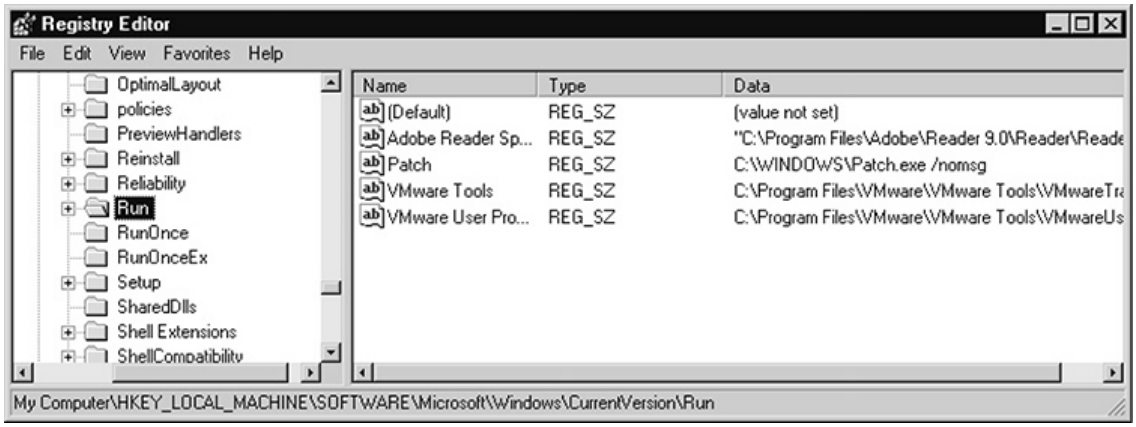


FIGURA 5-5

Quitar programas que están configurados para iniciarse automáticamente desde la parte Ejecutar del Registro

Otro software malintencionado

Además de los virus, hay otros tipos de software malicioso (conocido como malware) con el que debe estar familiarizado para el mundo real y para el examen de certificación Security+. En esta sección, aprenderá sobre spyware, adware y rootkits, por nombrar algunos de los tipos comunes de software malintencionado que amenazan los sistemas actuales.

Spyware

El spyware es un software oculto que monitorea y recopila información sobre usted y sus actividades y luego envía esa información a un sistema remoto para que el pirata informático la revise. Por ejemplo, el spyware podría recopilar información sobre sus hábitos de navegación. También se sabe que el spyware hace más que solo monitorear la información; También se sabe que realiza cambios en el sistema, como la redirección del navegador (que lo envía a una página web diferente) y ralentiza la conexión de red.

Adware

El adware es un software que carga automáticamente anuncios en la pantalla, generalmente en forma de una ventana emergente. El anuncio está diseñado para atraerlo a comprar un producto o suscribirse a un sitio.

Spam

Spam es el término utilizado para cualquier correo electrónico comercial no solicitado que reciba. Estos mensajes de correo electrónico suelen ser enviados por correo masivo e intentan que usted compre productos o servicios. Los spammers (personas que envían los mensajes de spam) generalmente obtienen su dirección de correo electrónico de un sitio web o grupo de noticias después de haber publicado un comentario en el grupo, o los spammers compran listas de correo electrónico en línea de compañías que han recopilado las direcciones de correo electrónico.

Los spammers utilizan programas automatizados, conocidos como *robots de spam,* para rastrear sitios web y recopilar cualquier dirección de correo electrónico que se haya publicado en ellos. Una vez que el spammer recopila suficientes direcciones de correo electrónico, busca negocios enviando un mensaje a todas las direcciones.

Las empresas pueden protegerse contra el spam al no publicar direcciones de correo electrónico en un sitio, o si es importante mostrar una dirección de correo electrónico, pueden hacerlo teniendo la dirección de correo electrónico en un archivo gráfico mostrado. Los robots de spam no

pueden recuperar la dirección de correo electrónico de un archivo gráfico porque no es texto en la página.

También puede proteger a su empresa de recibir mensajes de correo electrónico comerciales no solicitados configurando filtros de correo no deseado en sus servidores de correo electrónico (consulte **la Figura 5-6**) o utilizando un dispositivo antispam como Cisco IronPort o un servicio antispam en línea como Barracuda. La mayoría de los servidores de correo electrónico admiten los siguientes filtros de correo no deseado:

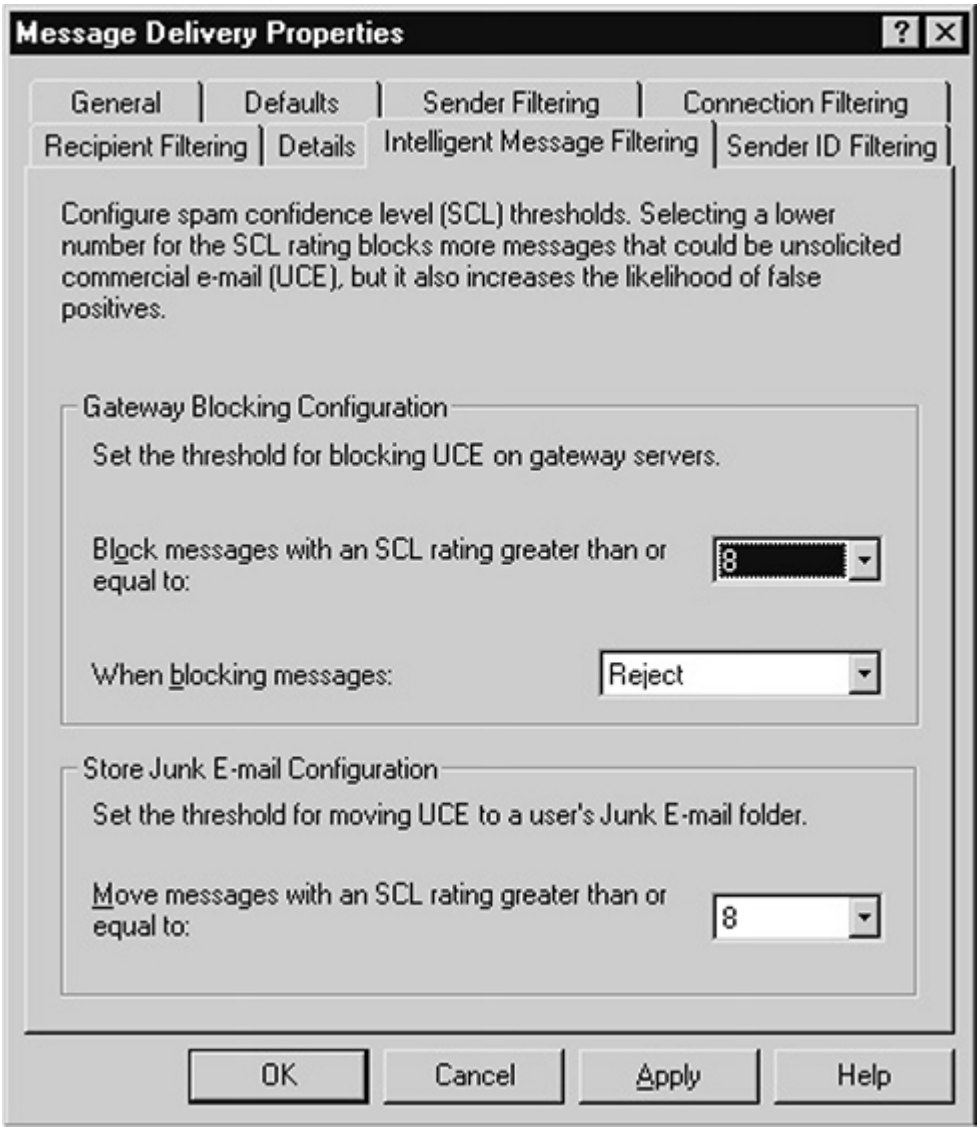


FIGURA 5-6

Observación de las opciones de filtrado de correo no deseado en un servidor de correo electrónico

■ Filtro de destinatarios Un filtro de **destinatarios** es una forma de bloquear un mensaje a un destinatario especificado (la línea Para en el encabezado del correo electrónico).

■ Filtro de remitente Un filtro de remitente puede bloquear un mensaje de un **remitente** especificado (la línea De en el encabezado del correo electrónico).

■ **Filtro** de conexión Un filtro de conexión es una lista de direcciones IP que tienen prohibido conectarse al servidor SMTP (Protocolo simple de transferencia de correo). Normalmente agregaría las direcciones IP de los servidores de correo que envían mensajes de spam (conocidos como hosts de spam) a un filtro de conexión.

■ Lista negra en tiempo real **(RBL)** No es práctico pensar que puede agregar todas las direcciones IP de todos los hosts de spam en Internet a su filtro de conexión, por lo que en su lugar puede suscribirse a una lista negra en tiempo real, que es una empresa que realiza un seguimiento de todos los hosts de spam en Internet.

■ **Filtro** de ID de remitente El filtro de ID de remitente permite que el servidor SMTP busque lo que se conoce como el registro SPF (Sender Policy Framework) en DNS de alguien que envía a los usuarios un mensaje de correo electrónico. El servidor SMTP comprueba el registro SPF del nombre de dominio que envía el correo electrónico y, si el servidor SMTP remitente aparece en el registro SPF, el servidor de correo aceptará el correo electrónico.

El spam es cuando alguien envía mensajes de correo electrónico no solicitados a un gran número de destinatarios. Puede proteger su empresa de los mensajes de spam implementando filtros en el servidor

de correo electrónico y no publicando direcciones de correo electrónico en Internet.

Rootkit

Un *rootkit* es un software instalado en un sistema por un hacker que normalmente está oculto para el administrador y le da al hacker acceso privilegiado al sistema. Estos son los cinco tipos principales de rootkits:

■ **Nivel de** aplicación Un rootkit a nivel de aplicación es un archivo ejecutable en modo usuario que le da al hacker acceso al sistema. Ejemplos de rootkits a nivel de aplicación son los virus troyanos.

■ **Nivel** de biblioteca Un rootkit a nivel de biblioteca no es un archivo ejecutable, sino más bien una biblioteca de código que puede ser llamada por una aplicación. Los rootkits de nivel de biblioteca son archivos DLL que se ejecutan en modo de usuario y, por lo general, reemplazarán una DLL en el sistema para ocultarse.

■ **Nivel de** kernel Un rootkit a nivel de kernel es un rootkit cargado por el kernel del sistema operativo y normalmente se planta en un sistema reemplazando un archivo de controlador de dispositivo en el sistema. Un rootkit a nivel de kernel se ejecuta en modo kernel en lugar de modo usuario, lo que significa que se ejecuta con más privilegios que un rootkit en modo usuario y, como resultado, tiene un mayor acceso al sistema y podría causar más daño.

■ Virtualizado Un rootkit **virtualizado** es un rootkit que se carga en lugar del sistema operativo cuando se inicia un sistema. Este rootkit luego carga el sistema operativo real en un entorno virtualizado. Estos rootkits son difíciles de detectar porque el sistema operativo no tiene idea de que se está alojando en el entorno virtualizado y porque no se ha reemplazado ningún código de aplicación o DLL en el sistema operativo.

■ **Firmware** Un rootkit de firmware se almacena en código de firmware en un sistema o dispositivo y es difícil de detectar porque no está presente en el sistema operativo.

Botnet

Una *botnet* es una colección de sistemas que han sido comprometidos por un hacker y que luego se utilizan para ayudar a realizar otros tipos de ataques. Los sistemas que están bajo el control del hacker en una botnet se conocen como *sistemas zombies*, o *bots,* porque no tienen mente propia y harán lo que el hacker ordene.

Para el examen Security+, sepa que una botnet es un grupo de sistemas controlados por un hacker para realizar ataques a sistemas a través de Internet.

La botnet se puede utilizar por varias razones, como correo electrónico no deseado o para realizar un ataque de denegación de servicio (DoS) en un objetivo específico. Una vez que un hacker tiene el control de muchos sistemas, el hacker puede alquilar los servicios de la botnet para realizar un ataque desde todos los sistemas de la botnet.

Troyano de acceso remoto

Un *troyano de acceso remoto (RAT)* es un software malicioso que el usuario suele instalar sin saberlo, como instalar un juego desde Internet o ejecutar un programa que se le envió por correo electrónico. El programa RAT luego abre una puerta trasera para que el atacante obtenga acceso al sistema de forma remota en un momento posterior. El malware RAT permite al atacante establecer una conexión con el sistema y ejecutar comandos de forma remota en ese sistema. Si un sistema en una red tiene una RAT en ejecución, es posible que el hacker pueda usar eso para comprometer otros sistemas, esencialmente creando una botnet.

Keylogger

Un keylogger es una pieza de software o un dispositivo de hardware que está diseñado para capturar todas las pulsaciones de teclas en un sistema. Como hardware, el keylogger es un pequeño dispositivo que se conecta al cable del teclado y luego a la computadora (consulte la **Figura 5-7**). Por lo general, el hacker entrará en una instalación y conectará el keylogger a un sistema. Una vez que el dispositivo está conectado entre el teclado y la computadora, cualquier pulsación de tecla en ese sistema se captura y almacena en el dispositivo. El hacker luego regresa para recuperar el dispositivo.

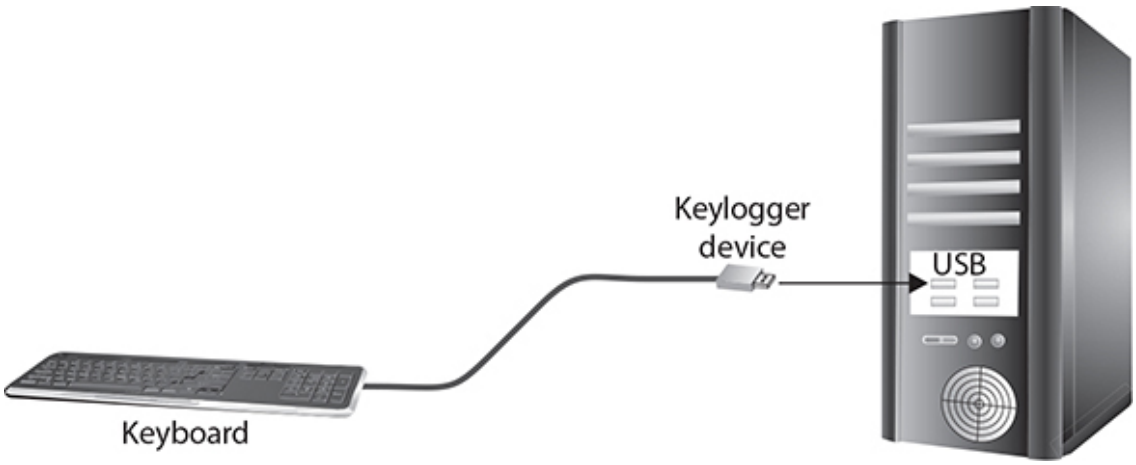


FIGURA 5-7

Un keylogger es una pieza de software o un dispositivo de hardware que registra las pulsaciones de teclas.

Un keylogger también puede ser una pieza de software instalada en el sistema. El software se ejecuta en segundo plano y captura todas las pulsaciones de teclas a un archivo en el disco duro o envía las pulsaciones de teclas a un sistema remoto. El hacker puede ver todas las palabras, por carácter, que se han escrito en el sistema. Esto permitirá al hacker ver datos confidenciales como nombres de usuario y contraseñas.

exam Watch

Para el examen, recuerde que una RAT es un software malicioso que permite a un atacante establecer una conexión con el sistema y eje-

cutar comandos remotos. También sepa que un keylogger es un software o hardware malicioso que registra las pulsaciones de teclas.

Puerta trasera

Cuando los hackers comprometen un sistema, generalmente instalan una *puerta trasera* en el sistema para que puedan acceder al sistema en un momento posterior. Los hackers instalan la puerta trasera porque saben que el método que utilizaron originalmente para comprometer el sistema puede ser bloqueado más tarde, por lo que crean un método alternativo para acceder al sistema. El hacker puede usar un virus troyano, abrir un puerto en el sistema con software o crear una cuenta de usuario en el sistema como puerta trasera que pueden usar más tarde para obtener acceso al sistema.

Ransomware

Otro tipo de software malicioso que se encuentra hoy en día es *el ransomware*. El ransomware es un malware común hoy en día que, cuando se ejecuta en su sistema, cifrará el contenido de su disco duro, y el pirata informático es el único con la clave de descifrado: esencialmente toman como rehenes sus datos hasta que pague el rescate. El hacker generalmente busca recibir el pago en bitcoin porque es más difícil de rastrear. Si decide no pagar, deberá borrar completamente el sistema y restaurar sus datos desde la copia de seguridad.

Programa potencialmente no deseado

El examen Security+ espera que comprenda el concepto de *programas potencialmente no deseados* o PUP para abreviar. Un PUP es un software que se instala en su sistema que no desea pero que se instaló porque se incluyó con otro programa que realmente quería e instaló. Los programas basura hacen muchas cosas molestas, como anuncios gráficos, instalar barras de herramientas, ralentizar potencialmente su computadora y pueden recopilar información privada sobre usted. Para ayudar a protegerse contra los programas basura, debe tener cuidado de vigilar cada pantalla al instalar software para asegurarse de que la opción para insta-

lar el software complementario esté desactivada y asegúrese de ejecutar software antimalware.

Virus sin archivos

Los virus sin archivos son malware que no instala ningún archivo en su sistema, sino que se ejecuta en la memoria del sistema. El malware generalmente se asocia con otro programa, de modo que cuando ejecuta ese programa, el malware se carga en la memoria y se ejecuta desde la memoria.

Comando y Control

El examen Security + también lo pondrá a prueba en comando y control (C&C), que es cuando un atacante compromete un sistema (o red de sistemas) y luego carga malware en él. Luego, el atacante utiliza un servidor de comando y control para enviar comandos a los sistemas que ejecutan el malware para que el atacante pueda realizar tareas como recuperar datos confidenciales de los sistemas e interrumpir la funcionalidad de los sistemas.

DENTRO DEL EXAMEN

Keyloggers como hardware o software

Recuerde para el examen Security+, y para el mundo real, que un keylogger puede ser un software instalado en el sistema por un hacker o un dispositivo de hardware que el hacker conecta al sistema entre el sistema y el teclado.

El keylogger de software generalmente captura las pulsaciones de teclas a un archivo en el sistema local, o puede enviar los datos a un archivo en un sistema remoto. El keylogger de hardware generalmente registra las pulsaciones de teclas en el

> dispositivo para que el pirata informático pueda recopilar el dispositivo en un momento posterior.

Cryptomalware

Cryptomalware es una forma de software malicioso que cifra los archivos del usuario sin el conocimiento del usuario y luego actúa típicamente como ransomware, informando al usuario que debe pagar una tarifa para descifrar sus archivos. El usuario suele ser engañado para instalar el cryptomalware en su sistema, y una vez que se instala, el software realiza el cifrado. Una vez que los archivos están encriptados por el software, el usuario no puede acceder a los archivos hasta que paguen el rescate y tengan los archivos desbloqueados.

Malware polimórfico y virus blindado

Otros dos tipos de malware con los que debe estar familiarizado para el examen de certificación Security+ son el malware polimórfico y los virus blindados. *El malware polimórfico* es un malware que se altera a sí mismo para evitar la detección del software antivirus que tiene una definición del malware. Debido a que el malware se ha mutado a sí mismo, hace que la definición en el software antivirus sea inútil.

Un virus *blindado* es un virus que se protege de ser analizado por profesionales de la seguridad. Es común que el personal de seguridad descompile el código del virus para comprender mejor cómo funciona el virus. Un virus blindado hace que sea difícil para alguien descompilar el programa y ver el código del virus.

Protección contra software malintencionado

Para el examen de certificación Security+, debe conocer los diferentes tipos de software malintencionado, pero también debe saber cómo protegerse contra el software malintencionado. La siguiente es una lista de contramedidas contra software malintencionado:

■ *Utilice software antivirus.* Asegúrese de que está utilizando software antivirus en todos los clientes y servidores de escritorio. Asegúrese de que el software antivirus admite protección en tiempo real que analizará los archivos y la memoria en busca de virus a medida que acceda a los datos.

■ *Mantenga actualizadas las definiciones de virus*. La base de datos de definición de virus es una lista de virus conocidos, y es fundamental mantener la base de datos actualizada para que su software de protección antivirus conozca los virus más recientes.

■ *Vigile de cerca los puertos de escucha*. Puede usar el comando **netstat** en Windows y Linux para ver una lista de puertos de escucha.

■ *Vigile de cerca los procesos en ejecución.* Puede utilizar el comando **tasklist** en Windows o el comando **ps -A** en Linux para ver una lista de procesos en ejecución. Es importante observar de cerca qué procesos se están ejecutando en segundo plano.

■ *Utiliza buenos hábitos de surf.* Eduque a los usuarios para que se mantengan alejados de sitios web desconocidos y para que no abran datos adjuntos recibidos en mensajes de correo electrónico de fuentes desconocidas.

Si está buscando algún software gratuito para ayudar a protegerse contra software malicioso o incluso para eliminar software malicioso, puede usar lo siguiente:

■ **Windows Defender** Este es un software de protección antivirus, protección contra spyware y protección contra malware que Microsoft incluye en todos los sistemas operativos compatibles. Al igual que otro software de protección antivirus, Windows Defender ofrece protección en tiempo real contra malware.

■ Herramienta de eliminación de software malintencionado de Microsoft Si tiene un sistema que ha sido infectado, puede descargar la Herramienta de **eliminación de software malintencionado de Microsoft**, que se actualiza regularmente. Es una gran herramienta para ayudar a eliminar el software malicioso de un sistema infectado.

Otro punto que debe hacerse es que si descubre que tiene un sistema infectado, no puede confiar en ningún software que se ejecute en ese sistema infectado, incluido el software antivirus. En esta situación, deberá arrancar desde un disco en vivo o una memoria USB que tenga su propio sistema operativo y software de protección antivirus. Una vez que arranque el sistema operativo en vivo, puede iniciar el software antivirus desde el sistema operativo en vivo para escanear el sistema y eliminar virus.

OBJETIVO DE CERTIFICACIÓN 5.04

Amenazas contra el hardware

No solo debe preocuparse por las amenazas del sistema, como el software malicioso, al proteger sus sistemas, sino que también debe preocuparse por las características relacionadas con el hardware de un sistema que debe protegerse. En esta sección, aprenderá acerca de las características de hardware populares para proteger correctamente un sistema.

Configuración del BIOS

El chip BIOS en una computadora contiene el código de bajo nivel que se utiliza para comunicarse con el hardware de un sistema. El código del BIOS también contiene lo que se conoce como el programa de *instalación CMOS*, que es un programa utilizado para configurar los ajustes de hardware en el sistema, como los tipos de memoria y unidades en el sistema y la fecha y hora en la computadora.

En lo que respecta a la seguridad, el programa de configuración CMOS (un ejemplo del cual se muestra en la **Figura 5-8**) se puede utilizar para

controlar desde qué dispositivos se pueden arrancar. Es una práctica recomendada de seguridad garantizar que los sistemas solo puedan arrancar desde el disco duro local y no desde la tarjeta de red, la unidad USB o una unidad de disco óptico que existe en el sistema. Es demasiado fácil para alguien usar un disco en vivo (una unidad USB o DVD que contiene un sistema operativo de arranque) para iniciar un sistema operativo en la memoria para obtener acceso al sistema. Para asegurarse de que esto no suceda, configure CMOS para que no permita el arranque desde nada más que el disco duro, si es posible.

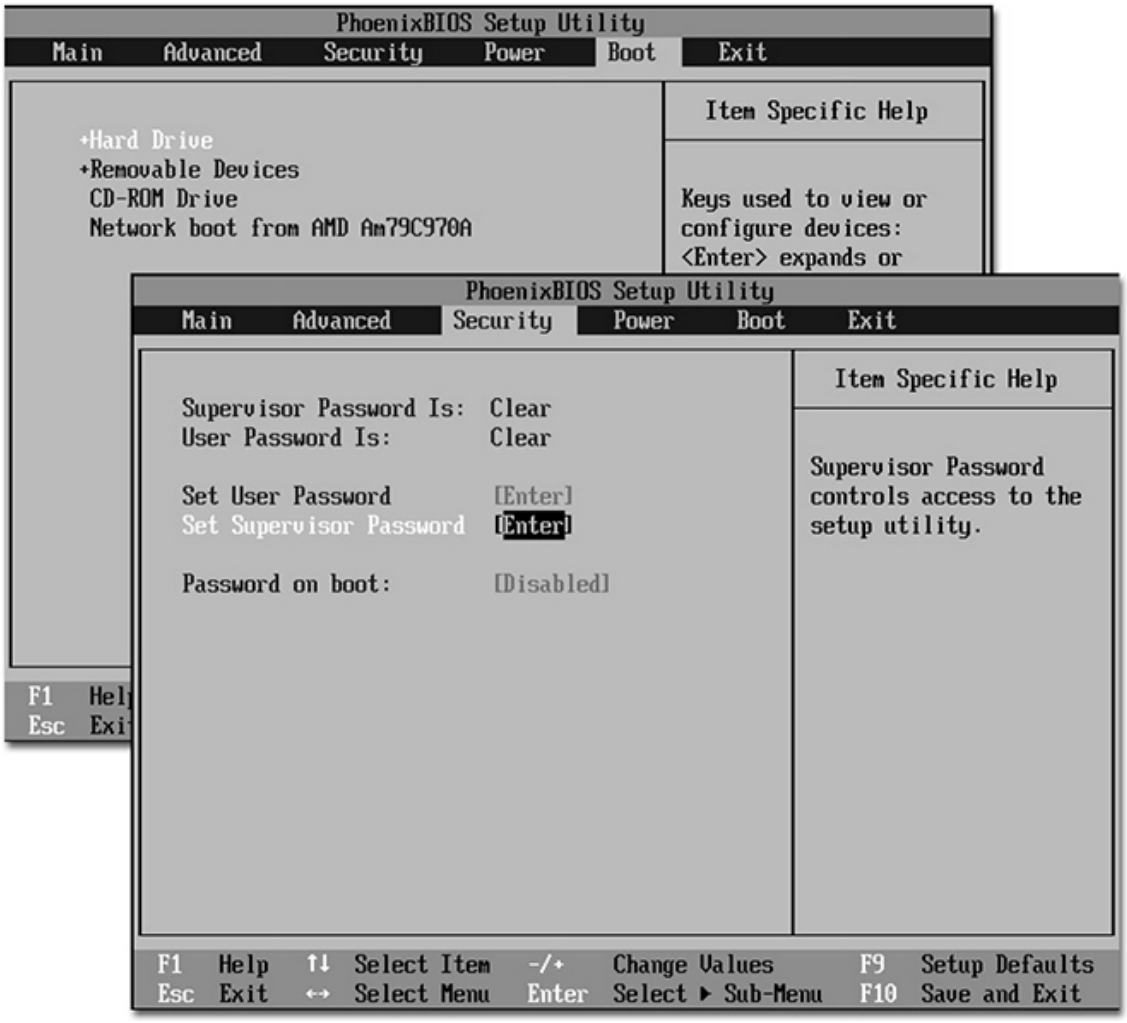


FIGURA 5-8

Uso de la configuración de CMOS para ayudar a proteger un sistema

En el programa de configuración de CMOS, también puede configurar una contraseña de "usuario", que es una contraseña necesaria para uti-

lizar el sistema. No confunda esta contraseña con la contraseña de Windows, ya que la contraseña CMOS aparece *antes* de que se cargue el sistema operativo. También asegúrese de configurar una contraseña de "administrador", que es una contraseña necesaria si alguien desea cambiar la configuración de CMOS.

Si le preocupa que las personas conecten dispositivos no autorizados a la computadora y potencialmente se lleven datos con ellos o comprometan el sistema a través del dispositivo no autorizado, debe asegurarse de que los puertos innecesarios estén deshabilitados a través del programa de configuración CMOS.

Dispositivos USB

Con respecto a los puertos, es importante actualizar su política de seguridad y educar a los usuarios sobre qué tipos de datos se pueden colocar en las unidades USB. Debido a que es fácil para los empleados llevar una copia de los datos con ellos en una unidad flash, la política de seguridad debe ser clara con respecto a qué tipos de datos se pueden colocar en las unidades USB. En entornos de alta seguridad, puede decidir que los puertos USB deben deshabilitarse para que no se puedan usar.

Debido a que se sabe que los virus de gusano se replican desde una memoria USB a un sistema, debería considerar deshabilitar los puertos USB en los sistemas de la oficina.

Uno de los riesgos importantes que rodean el uso de memorias USB es que un empleado podría tener un virus en su sistema en casa y colocar la unidad USB en su sistema, permitiendo que el virus gusano se replique en la memoria USB. El problema de seguridad con esto desde un punto de vista comercial es que si el empleado lleva la memoria USB a la oficina y la conecta a un sistema, el virus podría replicarse a los sistemas de trabajo.

Teléfonos inteligentes y tabletas

Los dispositivos móviles como teléfonos inteligentes y tabletas son dispositivos críticos en las operaciones comerciales actuales. La mayoría de los empleados reciben un teléfono o tableta como parte de su empleo, y es importante mantener seguros los datos en los dispositivos móviles. La mayoría de los teléfonos celulares de hoy en día se conocen como teléfonos inteligentes porque hacen más que hacer llamadas telefónicas. Almacenan información de contacto comercial y documentos confidenciales, y tienen planes de datos que permiten conexiones a Internet con el fin de revisar el correo electrónico y navegar por Internet.

Desde el punto de vista de la seguridad, asegúrese de que los empleados bloqueen sus teléfonos inteligentes y tabletas cuando no estén en uso y que estén cifrando los datos en estos dispositivos. Esto protegerá a la empresa de tener a alguien fuera de la empresa viendo datos confidenciales en el teléfono de un empleado si se pierde o es robado.

Como profesional de la seguridad, debe investigar las vulnerabilidades de todos los dispositivos móviles utilizados por los empleados de su empresa. Es importante estar familiarizado con todas las características de los dispositivos utilizados por su empresa y educarse sobre las diferentes vulnerabilidades que existen con cada uno de estos productos.

Debido a que la mayoría de los dispositivos móviles actuales usan Bluetooth, una tecnología inalámbrica que permite que un dispositivo Bluetooth se comunique con otro dispositivo Bluetooth a una distancia corta (hasta 30 pies), es fácil para los piratas informáticos comunicarse con su teléfono y robarle datos si Bluetooth está habilitado. Los teléfonos de hoy son vulnerables a varios ataques, incluidos los siguientes:

- **Bluesnarfing** Un exploit de Bluetooth que permite al hacker conectarse a un teléfono habilitado para Bluetooth y recuperar datos del teléfono

- **Bluejacking** El envío de mensajes no solicitados de un dispositivo Bluetooth a otro dispositivo Bluetooth

■ **Bluebugging** Un exploit de Bluetooth que implica que el hacker obtenga acceso al teléfono y aproveche todas sus capacidades, incluida la realización de llamadas utilizando el conjunto de comandos AT en el teléfono.

EJERCICIO 5-2

Explotación de un dispositivo Bluetooth

En este ejercicio, utiliza Kali Linux para aprender comandos relacionados con el concepto de bluesnarfing, el tipo de ataque que explota dispositivos Bluetooth como teléfonos inteligentes y tabletas.

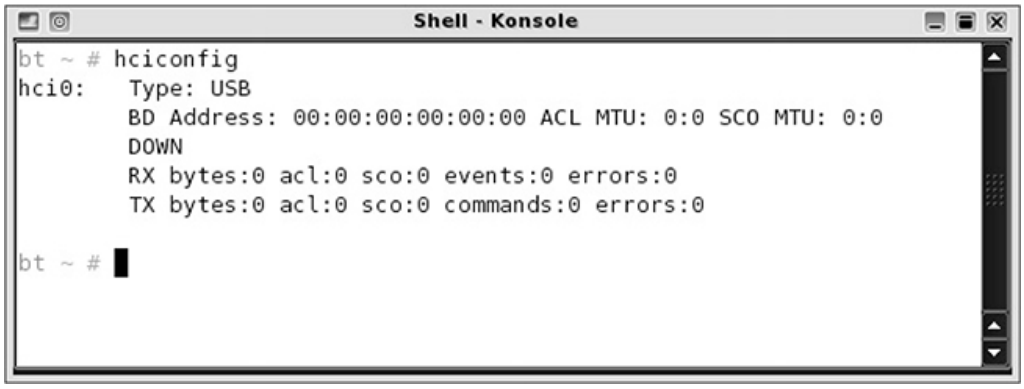
1. Asegúrese de que tiene Kali Linux ejecutándose con una tarjeta Bluetooth instalada.

2. Vaya al sistema Kali Linux e inicie una terminal.

3. Para ver una lista de sus adaptadores Bluetooth en Linux, escriba

```
hciconfig
```

4. Debería ver una lista de adaptadores Bluetooth instalados. Cada adaptador tiene un número de índice prefijado con *hci*. Por ejemplo, el primer adaptador es hci0, mientras que el segundo adaptador es hci1. Registre el número de adaptador: ____

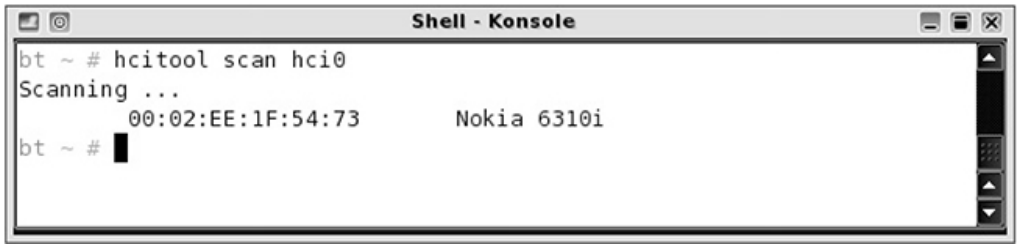


5. Al mirar el adaptador Bluetooth, debe notar la palabra "abajo" en la segunda línea. Esto significa que el adaptador está deshabilitado. Para habilitar el adaptador, escriba

```
hciconfig hci0 up
```

6. Una vez que tenga un dispositivo Bluetooth habilitado, puede comenzar a buscar otros dispositivos Bluetooth. Para buscar dispositivos Bluetooth cerca de usted, utilice la opción de **escaneo** en el comando **hcitool** y luego pase como parámetro el número de índice de su adaptador Bluetooth obtenido en el paso anterior. Para buscar dispositivos Bluetooth, escriba

```
hcitool scan hci0
```



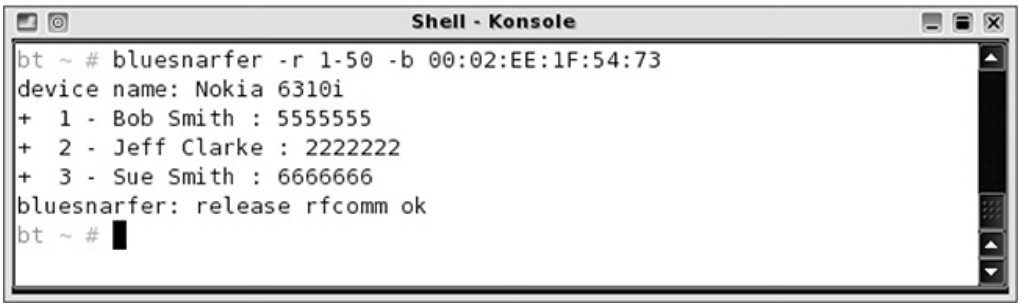
7. El escaneo debe informarle tanto de cualquier dispositivo Bluetooth cercano a usted como de la dirección MAC de ese dispositivo. Registre la dirección MAC del dispositivo Bluetooth que encontró: ____

8. Una vez que tenga la dirección MAC de un dispositivo Bluetooth, puede usar el comando **bluesnarfer** para recuperar información

sobre el dispositivo Bluetooth. Para ver la lista de direcciones en el teléfono, escriba

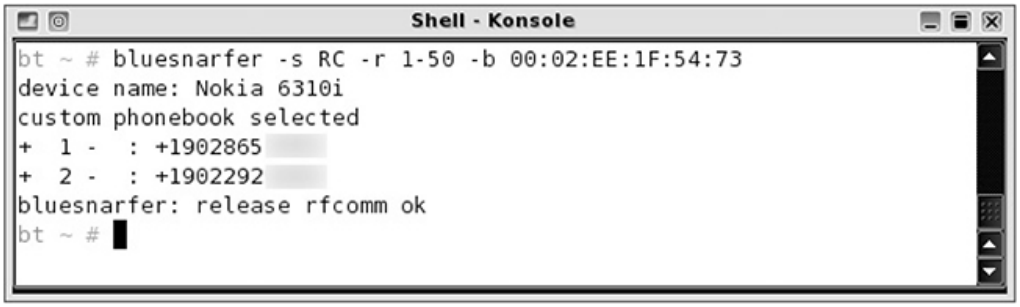
```
bluesnarfer -r 1-50 -b <mac of phone>
```

9. Tenga en cuenta que **-r** es para leer las entradas 1 a 50, y **-b** es el conmutador utilizado para especificar la dirección MAC del dispositivo a explotar.



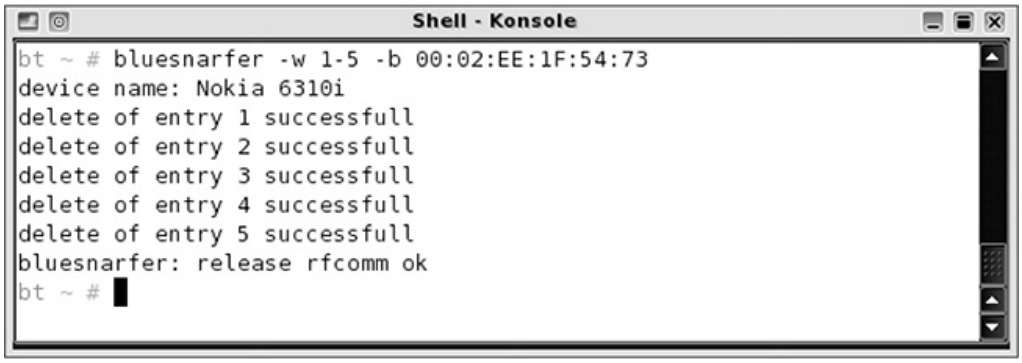
10. A continuación, puede utilizar el comando **bluesnarfer** para ver las llamadas recibidas en el teléfono escribiendo lo siguiente (tenga en cuenta que **RC** especifica que desea ver las llamadas recibidas):

```
bluesnarfer -s RC -r 1-50 -b <mac of phone>
```



11. Para eliminar las primeras cinco entradas de la libreta de direcciones con **bluesnarfer**, escriba

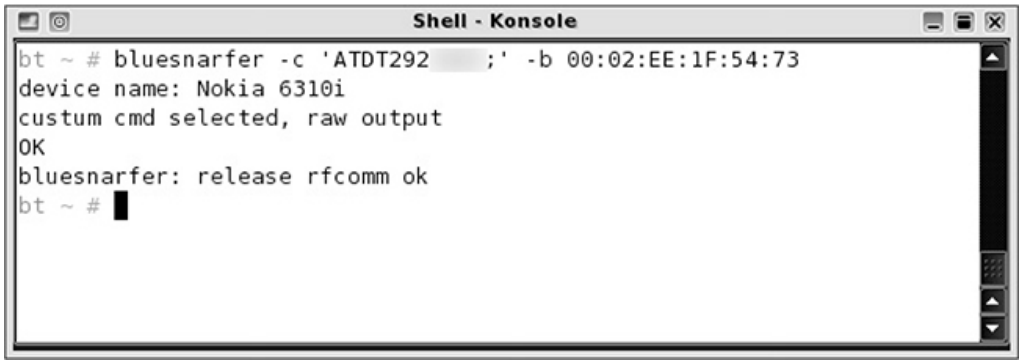
```
bluesnarfer -w 1-5 -b <mac of phone>
```



12. Para hacer una llamada telefónica usando el teléfono hackeado del sistema BackTrack, escriba

```
bluesnarfer -c 'ATDT#######;' -b <mac of phone>
```

13. Tenga en cuenta que **-c** especifica una acción personalizada y el comando **AT** marca un número, con el símbolo # actuando como marcador de posición para el número de teléfono.



14. ¿Cómo evitarías el bluesnarfing en tus dispositivos?

_____

_____

Cuando trabaje con dispositivos móviles requeridos por los usuarios, asegúrese de deshabilitar la funcionalidad Bluetooth si no es necesaria o si el empleado la utiliza. Si se requiere Bluetooth, configure la opción de visibilidad en deshabilitada o invisible para que otros dispositivos no puedan ver el dispositivo Bluetooth del empleado al escanear.

Para el examen, sepa que *bluesnarfing* es la recuperación no autorizada de datos de un dispositivo Bluetooth y que *bluejacking* es el envío de mensajes no solicitados de un dispositivo Bluetooth a otro.

La mayoría de los dispositivos Bluetooth actuales utilizan seguridad emparejada, lo que significa que otro dispositivo Bluetooth no puede conectarse a su dispositivo Bluetooth sin antes solicitarle un número PIN, que actúa como código de acceso. Si la persona que se conecta ingresa el mismo número PIN, entonces la conexión está permitida.

Almacenamiento extraíble

Es importante incluir en su política de seguridad las reglas que rodean el almacenamiento *extraíble,* que es cualquier medio de almacenamiento que puede almacenar datos y luego eliminarse del sistema. Por ejemplo, las unidades flash (también conocidas como memorias USB) y las unidades de disco duro externas conectadas a un sistema mediante USB, FireWire o eSATA se consideran almacenamiento extraíble.

El problema de seguridad que rodea el almacenamiento extraíble es que un empleado podría traer una unidad de memoria de casa y conectarla al sistema de la empresa. Esto es un problema porque algunos virus de gusano pueden infectar los sistemas de la empresa al replicarse desde la unidad extraíble al sistema de la empresa. Es mejor no permitir que los empleados utilicen almacenamiento extraíble en la red de la empresa y asegurarse de que la política de seguridad lo especifique.

Si la empresa suministra dispositivos de almacenamiento extraíbles a los empleados para almacenar información de la empresa, asegúrese de que las unidades sean capaces de cifrar los datos almacenados en la unidad. Es muy fácil para los empleados extraviar la unidad extraíble o que se la roben, así que asegúrese de tener los datos confidenciales encriptados en las unidades.

Por último, algunos entornos de alta seguridad tienen discos duros extraíbles en las estaciones de trabajo. Estas organizaciones tienen una política de que cuando un empleado sale de una estación, debe sacar la unidad del sistema y luego bloquearla en un gabinete seguro. Este también puede ser el caso de las computadoras portátiles utilizadas por los empleados. Es posible que se requiera que los empleados bloqueen sus computadoras portátiles en un gabinete seguro cuando se vayan por el día. El beneficio es que si alguien, como el personal de limpieza, tiene acceso a las instalaciones por la noche, entonces las unidades o computadoras portátiles se almacenan de forma segura.

Almacenamiento conectado en red

Un dispositivo de almacenamiento conectado a la red (NAS) es un dispositivo que se conecta a la red y tiene un grupo de unidades instaladas. Las unidades normalmente se configuran en una solución tolerante a errores, como una matriz RAID, y permiten que los clientes de la red se conecten directamente al dispositivo.

El NAS proporciona una ubicación central para compartir archivos con clientes en la red y admite diferentes tipos de clientes (Linux y Windows) que se conectan al NAS para acceder a los archivos. Esto es posible porque el dispositivo NAS ejecuta la mayoría de los protocolos de uso compartido de archivos, como Server Message Block (SMB) para clientes Windows y Network File System (NFS) para clientes Linux.

Una vez que conecte el NAS a la red, puede modificar sus opciones de configuración a través de una interfaz basada en web.

Tenga mucho cuidado al proteger los datos en un dispositivo NAS porque todos los datos de la empresa ahora podrían almacenarse en esa ubicación. Las siguientes son algunas consideraciones a tener en cuenta cuando se trata de NAS:

■ *Comprometer el acceso afecta a todos los datos.* Si alguien puede obtener acceso al NAS, potencialmente tendrá acceso a todos los datos en el NAS.

Para controlar el acceso al dispositivo NAS, asegúrese de tener un firewall que separe el dispositivo NAS de Internet.

- *Un virus podría infectar potencialmente todos los archivos.* Debido a que todos sus datos se almacenan en una ubicación, es posible que un virus se propague a través de todos sus datos. Asegúrese de realizar análisis de virus regulares en los datos almacenados en el NAS.

- *Implementar lo básico.* Utilice la autenticación, los permisos y el cifrado cuando sea posible en el dispositivo NAS para controlar quién tiene acceso a los datos del dispositivo.

PBX

Una central de sucursal privada (PBX) es un sistema telefónico avanzado que actúa como un interruptor para todos los teléfonos dentro de la corporación. El PBX permite a una empresa comprar una sola línea externa y luego tener múltiples sistemas telefónicos internos (y números) dentro de la empresa que utilizan el PBX. A cada teléfono de la empresa se le asigna un número único, que actúa como el número de extensión de la línea externa (consulte la **Figura 5-9**).

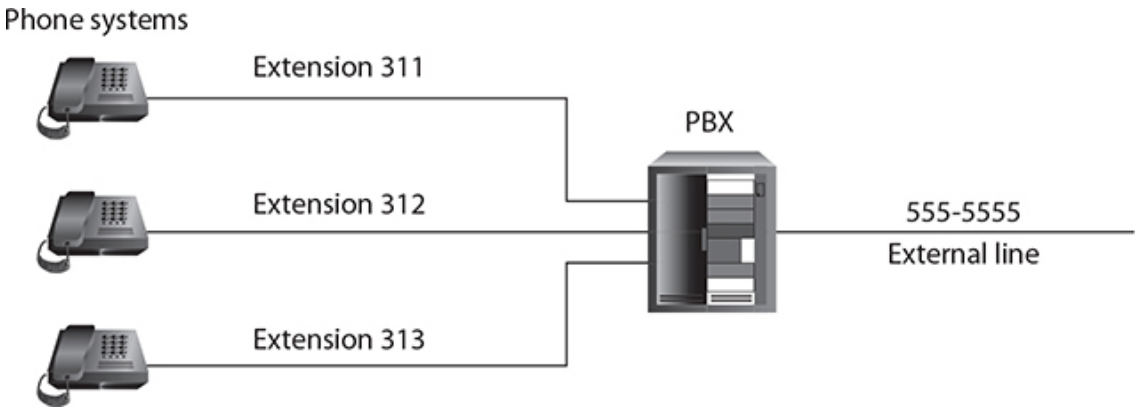


FIGURA 5-9

Una PBX actúa como un interruptor para el sistema telefónico dentro de una empresa.

Debido a la naturaleza de los sistemas telefónicos, normalmente una serie de problemas de seguridad están relacionados con las PBX. El primer punto clave es controlar quién tiene acceso a la PBX colocándola en una habitación cerrada con acceso limitado. Asegúrese de que los componentes de hardware de la PBX estén en una ubicación segura y considere el uso de dispositivos antimanipulación para ayudar a proteger la PBX. Al evaluar la seguridad, asegúrese de revisar los componentes de hardware regularmente para asegurarse de que no hayan sido manipulados.

Al igual que con cualquier dispositivo, asegúrese de modificar cualquier configuración predeterminada en el PBX cuando sea posible, incluidas las cuentas y contraseñas predeterminadas. Además, si se requiere administración remota en el PBX, asegúrese de implementar la seguridad de devolución de llamada, donde el sistema se desconecta de la conexión original y luego se conecta a un número predefinido. Esto asegurará que un hacker no esté tratando de conectarse remotamente a la PBX.

Asegúrese de que los usuarios no estén conectando módems a las líneas telefónicas de la empresa, ya que esto crea el riesgo de que una persona no autorizada marque ese número y luego obtenga acceso remoto a la red interna (¡eso no es bueno!). El término para alguien que marca varios números para localizar un módem conectado a un número es *marcación de guerra.* Uno de los escenarios comunes para la marcación de guerra hace años era cuando los administradores tenían un módem conectado a la PBX para fines de administración remota. El hacker localizaría el PBX a través de la marcación de guerra y luego obtendría acceso al PBX para hacer llamadas de larga distancia a través del PBX.

No confunda la marcación de guerra con la conducción de guerra. *La marcación* de guerra es cuando el hacker llama a varios números con la esperanza de localizar un módem conectado a una línea telefónica, mientras que la *conducción de guerra* es cuando el

hacker usa un escáner inalámbrico para localizar redes inalámbricas.

Riesgos de seguridad con sistemas integrados y especializados

En esta sección aprenderá sobre técnicas comunes para mitigar riesgos en entornos que utilizan diferentes tipos de tecnologías. Para mitigar los riesgos, debe comprender las tecnologías y sus riesgos de seguridad relacionados.

El principal desafío para mitigar las amenazas de seguridad es la riqueza de los diferentes productos y tecnologías utilizados por las organizaciones hoy en día. Como profesional de la seguridad, debe crear, o al menos aconsejar cómo crear, un entorno seguro para cada una de estas tecnologías y sistemas especializados.

Sistemas embebidos

Esté atento a los dispositivos que tienen componentes integrados que podrían crear riesgos. Esto incluye cualquier dispositivo conectado a la red, como una impresora o un televisor inteligente, pero también esté atento a los dispositivos que incluyen tecnología Bluetooth. Asegúrese de implementar prácticas de endurecimiento con estos dispositivos (por ejemplo, si el dispositivo no usa Bluetooth, debe deshabilitarse, si es posible):

- **Raspberry Pi Raspberry Pi** es una pequeña placa de sistema que contiene un procesador; CARNERO; y puertos como puertos USB, Micro HDMI y un puerto Gigabit Ethernet. Estos pequeños sistemas son comunes con los usuarios domésticos y se utilizan para crear dispositivos personalizados que proporcionan algún tipo de funcionalidad.

- Matriz de puertas **programables en campo (FPGA) Una matriz de puertas programable en campo** es un circuito integrado que se envía al cliente para que el cliente pueda programar su propia funcionalidad en el chip.

■ **Arduino Arduino** es un producto popular que los clientes utilizan para crear sus propios dispositivos electrónicos. Arduino viene con una pequeña placa que contiene microprocesadores y controladores que se pueden programar con lenguajes como C y C ++.

Otras tecnologías integradas

Existen otras tecnologías que funcionan con sistemas integrados o tienen componentes integrados en ellos. La siguiente es una lista de otras tecnologías relacionadas a tener en cuenta:

■ HVAC El sistema **HVAC** tiene un sistema informático integrado para detectar y controlar la temperatura del ambiente.

Un sistema en chip (SoC) es esencialmente un sistema informático en un chip de computadora que está incrustado en placas. Los SoC pueden contener una gran cantidad de funcionalidades, incluidas CPU, GPU y módulos inalámbricos. Un ejemplo de un dispositivo que utiliza un SoC es Raspberry Pi.

■ RTOS Un sistema operativo en tiempo real (**RTOS**) es un sistema operativo que se encuentra en un sistema integrado que está diseñado para procesar datos a medida que llegan al dispositivo.

■ **Impresoras**/MFD Las impresoras y los dispositivos multifunción (MFD, que son dispositivos que funcionan como impresora, fax y escáner) tienen una serie de componentes integrados que debe tener en cuenta. Por ejemplo, tienen memoria para almacenar información, algunas impresoras tienen discos duros que potencialmente almacenan trabajos de impresión (que podrían contener información confidencial), y muchas impresoras también son servidores web, lo que las hace fácilmente explotadas.

■ **Sistemas de vigilancia** Los sistemas de vigilancia actuales contienen sistemas integrados. Al igual que con las impresoras, debe conocer los ele-

mentos electrónicos en los sistemas de cámaras, pero también debe conocer los sistemas que contienen cámaras. También tenga en cuenta que muchas cámaras están conectadas a un servidor central que podría controlar las cámaras y / o es donde las cámaras envían sus datos. Estos sistemas pueden estar conectados a Internet, por lo que una vulnerabilidad expondría la vista de la cámara a cualquier número de personas.

- **Drones** Un dron es un vehículo aéreo no tripulado (UAV) que implica que el piloto de la aeronave pueda volar el dron con un control remoto.

- VoIP Voz sobre Protocolo de Internet (**VoIP**) es una tecnología que nos permite utilizar una red TCP/IP, como Internet, para llevar aplicaciones de comunicación de voz y conferencias.

- **Consolas de juegos** Los sistemas de juego actuales, como Xbox y PlayStation, son ahora sistemas multimedia completos conectados a Internet. Asegúrese de mirar las técnicas de endurecimiento en estos sistemas y realizar actualizaciones en ellos regularmente.

SCADA/ICS

El control de supervisión y adquisición de datos (SCADA) es un sistema especial utilizado en entornos industriales (por ejemplo, una planta de fabricación) para monitorear las operaciones. Los sistemas SCADA son utilizados por los gerentes de instalaciones para manejar la logística relacionada con el control de componentes como HVAC, iluminación y unidades de refrigeración. La seguridad física, incluida una instalación segura, es una parte importante de la seguridad en dicho entorno, ya que cualquier manipulación de cualquiera de los componentes SCADA puede causar un mal funcionamiento del monitoreo y las alarmas. *El sistema de control industrial (ICS)* se refiere generalmente a cualquier sistema que monitoree o controle equipos industriales, incluidos los sistemas SCADA. Estos sistemas se pueden encontrar en muchos tipos de instalaciones, incluidas plantas industriales, plantas de fabricación y plantas de energía.

Internet de las cosas

Internet de *las cosas (IoT)* es el término que utilizamos para los dispositivos que pueden intercambiar información a través de Internet con otros dispositivos y sistemas. Un dispositivo IoT podría ser vulnerable a los ataques, ya que los proveedores de los productos generalmente se centraban en la comunicación y no en la seguridad cuando se creó el producto. Los siguientes objetivos de Security+ son puntos clave para recordar sobre IoT:

- **Sensores** Muchos dispositivos IoT tendrán sensores que le permitirán recopilar información. Algunos ejemplos de dispositivos IoT que contienen sensores son electrodomésticos como termostatos y cámaras de seguridad para el hogar.

- **Dispositivos inteligentes** Un dispositivo inteligente es un dispositivo que está conectado a la red o a Internet y es capaz de comunicarse con otros dispositivos. Estos dispositivos generalmente se conectan a la red o a Internet mediante tecnologías inalámbricas como Bluetooth, Wi-Fi o una red celular.

Un wearable es un dispositivo electrónico como un reloj inteligente que puedes usar en tu cuerpo. Por ejemplo, un reloj inteligente es capaz de comunicarse con un teléfono inteligente a través de Bluetooth. Los wearables pueden actuar como un monitor de fitness y un monitor de frecuencia cardíaca.

- **Automatización** de instalaciones Los sistemas de automatización de instalaciones están diseñados para controlar elementos dentro del edificio, como calefacción, ventilación y aire acondicionado (HVAC).

- **Valores predeterminados débiles** Muchos dispositivos de Internet de las cosas pueden tener configuraciones predeterminadas que hacen que los dispositivos no sean seguros. Es fundamental que revise su configuración

predeterminada y modifique la configuración de los valores predeterminados tanto como pueda, ¡ya que la configuración predeterminada es lo que los piratas informáticos saben!

Sistemas Especializados

Hay una serie de sistemas de propósito especial que contienen sistemas integrados, incluidos dispositivos médicos, vehículos y sistemas de aeronaves / UAV. Cada uno de estos sistemas debe ser evaluado para detectar vulnerabilidades.

- Sistemas informáticos en el vehículo Si su organización tiene sistemas **informáticos en** los vehículos, asegúrese de implementar controles de seguridad especiales para esos sistemas, además de las prácticas de seguridad regulares. Por ejemplo, si los vehículos de la empresa están equipados con computadoras portátiles, asegúrese de cifrar los datos en el disco, implementar un control de bloqueo que proteja el dispositivo de ser robado y deshabilitar puertos y tarjetas de red innecesarios en la computadora portátil. Los automóviles de hoy en día tienen sistemas de comunicación como OnStar que están conectados al automóvil vía satélite y permiten al fabricante proporcionar muchas funciones, como llamadas de emergencia. El posible problema de seguridad es que un hacker puede explotar el sistema y controlar el automóvil.

- **Sistemas** médicos Los sistemas médicos tienen sistemas informáticos integrados que tienen conectividad de red utilizada para recopilar y transferir datos médicos.

- **Vehículos** Los fabricantes de vehículos están utilizando la tecnología IoT para que los vehículos estén en constante comunicación con los sistemas informáticos de los fabricantes. Los fabricantes utilizan los datos recopilados de estos vehículos para mejorar las características y hacer que los vehículos sean más seguros. Este canal de comunicación también se utiliza para actualizar el software de los vehículos cuando los fabricantes necesitan implementar actualizaciones de software.

■ **Aeronaves** Similar a la tecnología IoT en los automóviles, las aerolíneas también están utilizando IoT en los aviones para que puedan recopilar información sobre los aviones y sus vuelos.

■ **Medidores inteligentes Los medidores inteligentes** son dispositivos que recopilan información sobre el consumo de energía para que la compañía eléctrica pueda controlar mejor su consumo de energía.

Consideraciones de comunicación

Los sistemas integrados y los dispositivos IoT utilizarán diferentes métodos de comunicación para enviar los datos recopilados al sistema del fabricante. Al determinar el riesgo para los dispositivos IoT utilizados por la empresa, no olvide investigar la tecnología de comunicación utilizada y las vulnerabilidades en el canal de comunicación. Las siguientes son tecnologías de comunicación utilizadas por estos dispositivos:

■ Los sistemas integrados 5G y los dispositivos IoT pueden usar redes celulares para transmitir la información recopilada al fabricante, siendo el estándar actual la red celular de quinta generación (**5G**).

■ Los dispositivos de banda estrecha pueden utilizar canales de comunicación de radio de **banda estrecha** para la comunicación de corto alcance. Por ejemplo, la tecnología RFID y la entrada remota sin llave con vehículos suelen utilizar una banda estrecha.

■ Radio de banda base La radio de **banda base** es una tecnología de comunicación que utiliza ondas de radio para enviar una señal entre dos puntos.

■ **Tarjetas de módulo de identidad del suscriptor (SIM)** Una tarjeta SIM es un pequeño chip de computadora colocado en un teléfono celular que almacena la información necesaria para conectarse a la red celular.

También puede almacenar datos personales como mensajes y contactos en la tarjeta SIM.

- Zigbee **Zigbee** es un protocolo de comunicación utilizado para crear una red de área personal (PAN) entre dispositivos tales como sistemas de automatización del hogar o equipos de dispositivos médicos.

Restricciones

Las siguientes son algunas limitaciones potenciales que puede experimentar al trabajar con sistemas integrados o dispositivos IoT:

- **Los** dispositivos Power IoT necesitarán usar energía para crear una señal lo suficientemente fuerte como para enviar datos. Los fabricantes deben asegurarse de que los componentes reciban suficiente energía para una funcionalidad estable del componente.

- **Cómputo** El componente deberá tener la potencia de cálculo para procesar la información recopilada.

- **Red** La red debe ser eficiente y fiable para poder transmitir los datos recogidos.

- **Crypto** Para asegurar la comunicación, la tecnología utilizará algún tipo de algoritmo de criptografía para cifrar las comunicaciones. Para el examen, recuerde estar atento a las soluciones que utilizan algoritmos de cifrado débiles como DES y 3DES. Aprenderá más sobre el cifrado en **los capítulos 12** y **13**.

- Incapacidad para parchear Otro punto clave con los dispositivos IoT para recordar para el examen que es una gran limitación o vulnerabilidad es un dispositivo que no da la capacidad de aplicar actualizaciones (**parchear** el sistema). Si un dispositivo no proporciona una forma de aplicar

parches, eso significa que las vulnerabilidades encontradas dentro del dispositivo siempre existirán.

- **Autenticación** Mire los protocolos de autenticación compatibles con el dispositivo y asegúrese de que, si puede elegir un protocolo de autenticación, utilice el protocolo más seguro posible (uno que admita el tráfico de autenticación cifrado).

- **Alcance** El alcance de la tecnología también puede ser una limitación. Por ejemplo, Bluetooth 4.2 tiene un alcance limitado de 60 metros, mientras que Zigbee tiene un alcance máximo de 100 metros.

- **Coste** El coste de la tecnología integrada podría aumentar el coste del componente para el cliente.

- **Confianza** implícita La tecnología puede seguir la regla de la confianza implícita, donde confía en toda comunicación.

RESUMEN DE CERTIFICACIÓN

En este capítulo aprendió acerca de algunos de los tipos más comunes de amenazas contra los sistemas actuales. Ha aprendido sobre las amenazas físicas a los activos, como el robo de dispositivos, y sobre las amenazas de software y hardware malintencionadas. Los siguientes son algunos puntos clave para recordar acerca de las amenazas de seguridad del sistema:

- La mayoría de las empresas centran su estrategia de TI en la tecnología; Sin embargo, no deben olvidarse de las amenazas de seguridad física, como el espionaje y el robo de hardware.

- Una política de escritorio limpio y garantizar que los empleados estén destruyendo documentos innecesarios ayudará a evitar el espionaje.

■ Asegúrese de proteger con contraseña cualquier dispositivo móvil y también cifre los datos en esos dispositivos en caso de que se pierdan o sean robados.

■ Familiarizarse con los diferentes tipos de software malicioso, como virus, spyware y adware.

■ Asegúrese de proteger su sistema del software malicioso instalando software de protección antivirus y manteniendo actualizadas las definiciones de virus. Puede utilizar comandos del sistema operativo como **netstat**, **tasklist** y **taskkill** para supervisar lo que se está ejecutando en el sistema.

■ Asegúrese de que los usuarios estén cifrando todos los datos almacenados en unidades extraíbles en caso de pérdida o robo de una unidad extraíble, esto incluye unidades USB. Asegúrese también de controlar qué unidades se pueden conectar a los sistemas corporativos; No desea que una memoria USB que fue infectada con un virus de la computadora doméstica de un empleado ingrese a su red.

■ Cuando obtenga nuevos dispositivos, como teléfonos inteligentes en la oficina, asegúrese de investigar las características de estos dispositivos y deshabilite lo que no se está utilizando, como Bluetooth. Además, investigue las vulnerabilidades de estos dispositivos en particular.

Comprender las amenazas contra un sistema es una habilidad importante para tener como profesional de seguridad y lo ayudará a responder preguntas relacionadas en el examen. Siempre tenga una mente sospechosa cuando se trata de seguridad, y con cualquier nueva tecnología, pregúntese: "¿Cuáles son las amenazas contra esto?"

✓ SIMULACRO DE DOS MINUTOS

Problemas de seguridad con vulnerabilidades

❑ Esté atento a la configuración débil de los dispositivos de software o hardware que podrían hacer que el sistema sea vulnerable a un ataque. Ejemplos de configuración débil son la falta de permisos que controlan las acciones autorizadas, el cifrado débil (como el uso de DES o 3DES) y el uso de protocolos no seguros (como HTTP en lugar de HTTPS).

❑ Recuerde modificar la configuración de los valores predeterminados del sistema, ya que los hackers conocen los valores predeterminados de los sistemas que atacan.

❑ Asegúrese de aplicar parches al sistema regularmente. Esto incluye actualizaciones de firmware, actualizaciones del sistema operativo y cualquier actualización de la aplicación para el software que esté ejecutando.

❑ Debe deshabilitar los puertos USB en los sistemas o implementar DLP para evitar la exfiltración de datos.

Identificación de amenazas físicas

❑ Asegúrese de que los empleados destruyan los documentos confidenciales cuando se deshagan de ellos para ayudar a prevenir técnicas de espionaje como el buceo en contenedores de basura.

❑ Implemente una política de escritorio limpio, especificando que los documentos confidenciales no pueden dejarse a la intemperie.

❑ Asegúrese de que los empleados estén bien educados sobre las tareas del trabajo para ayudar a prevenir errores humanos, como la eliminación accidental de archivos o la destrucción de equipos informáticos debido a ESD.

❑ Cifre y asegure los dispositivos con contraseñas para proteger los datos de la empresa que residen en un dispositivo en caso de pérdida o robo.

Mirando el software malicioso

❑ La escalada de privilegios es cuando un usuario puede obtener acceso administrativo a un sistema explotando una vulnerabilidad en el sistema.

❑ Una bomba lógica es un tipo de virus que se desencadena por un evento específico, como una fecha.

❑ Un virus gusano es un virus autorreplicante y se replica a través de unidades flash, correo electrónico o a través de la red para infectar sistemas.

❑ Un virus troyano es un virus que se instala pensando que el programa es un programa legítimo, pero en su lugar le da al pirata informático acceso al sistema (generalmente abriendo un puerto en su computadora).

❑ Puede usar comandos del sistema operativo como **netstat**, **tasklist** y **taskkill** para ayudar a solucionar problemas de sistemas infectados con software malintencionado. También puede consultar la Herramienta de eliminación de software malintencionado de Microsoft para eliminar el malware de un sistema infectado.

❑ El spyware es un software que recopila información sobre sus hábitos de navegación, mientras que el adware es un malware que carga anuncios en la pantalla en una ventana emergente.

❑ Los mensajes de spam son correos electrónicos no solicitados enviados masivamente anunciando un producto o servicio.

❑ Un rootkit es una pieza de software instalada por un hacker que les otorga acceso administrativo al sistema más tarde. Los diferentes tipos son rootkits virtualizados y a nivel de aplicación, nivel de biblioteca, nivel de kernel y virtualizados.

❑ Un keylogger es una pieza de software o hardware que captura las pulsaciones de teclas y las almacena en un archivo para que el hacker las revise más tarde.

Amenazas contra el hardware

❑ Debe configurar los ajustes del BIOS en todas las estaciones de trabajo y servidores para que los sistemas no arranquen desde una unidad de arranque, como una unidad USB o una unidad de DVD que contenga un sistema operativo de arranque.

❑ Asegúrese de desactivar los puertos no utilizados en un sistema, como los puertos USB, para evitar que los empleados se lleven datos confidenciales a casa, o incluso que introduzcan un virus en el sistema a través de una unidad USB.

❑ Asegúrese de investigar cualquier vulnerabilidad conocida con teléfonos móviles y de deshabilitar funciones innecesarias en el teléfono.

❑ Bluesnarfing es la explotación de un dispositivo Bluetooth copiando datos del dispositivo, mientras que bluejacking es el envío de mensajes no solicitados a un dispositivo Bluetooth.

❑ Limitar el uso de medios extraíbles en el lugar de trabajo para reducir la probabilidad de robo intelectual. Si va a utilizar medios extraíbles, tenga los datos de la unidad cifrados en caso de que los medios se pierdan o sean robados.

AUTOEVALUACIÓN

Las siguientes preguntas le ayudarán a medir su comprensión del material presentado en este capítulo. Como se indicó, algunas preguntas pueden tener más de una respuesta correcta, así que asegúrese de leer todas las opciones de respuesta cuidadosamente.

Problemas de seguridad con vulnerabilidades

1. Su gerente ha leído acerca de que la exfiltración de datos es una preocupación importante para las empresas de hoy. Ella se ha acercado a usted buscando métodos para reducir el riesgo de exfiltración de datos. ¿Qué me recomiendas?

A. Instale software antivirus.

B. Desactive los puertos USB.

C. Habilite Firewall de Windows.

D. Desactivar servicios innecesarios.

2. Su gerente le ha pedido que implemente una solución que impida que los empleados envíen correo electrónico fuera de la empresa que contenga información confidencial. ¿Qué solución recomendaría?

A. NAT

B. NAC

C. DES

D. DLP

3. Ha estado leyendo un nuevo boletín de seguridad que describe una nueva vulnerabilidad dentro de uno de los sistemas operativos que uno de sus servidores web críticos está ejecutando. ¿Qué debe hacer para reducir el riesgo de un exploit en ese sistema crítico?

R. Utilice HTTPS en lugar de HTTP.

B. Bloquee los permisos.

C. Parche el sistema.

D. Habilite un firewall basado en host.

Identificación de amenazas físicas

4. Su gerente de ventas se ha puesto en contacto con usted para informarle que recientemente extravió su dispositivo móvil, que puede contener información confidencial. ¿Qué debe indicarle que haga primero?

A. Solicite uno nuevo.

B. Borre el dispositivo de forma remota.

C. Llame al teléfono y pida que se lo devuelvan.

D. Desactive Bluetooth en el dispositivo.

5. Estás planificando tus seminarios de formación y sensibilización. ¿Qué debe decirles a los empleados que hagan con los documentos confidenciales que ya no son necesarios?

A. Guárdelos en una pila en el lado derecho de su escritorio.

B. Colóquelos en la bolsa de la computadora portátil cuando ya no los necesite.

C. Destrozarlos.

D. Colóquelos en la papelera de reciclaje para su reciclaje.

6. A su gerente le preocupa que las computadoras portátiles de los empleados sean robadas a la mitad del día cuando los empleados salen de su escritorio para tomar café o ir al baño. ¿Qué puede hacer para reducir la probabilidad de que un transeúnte tome una computadora portátil dejada en un escritorio?

A. Utilice un cable de bloqueo.

B. Cifre la unidad.

C. Desactive el arranque desde un disco en vivo.

D. Cierre la sesión de la estación de trabajo.

Mirando el software malicioso

7. Su empresa tiene una política estricta cuando se trata del uso de unidades USB en la oficina. Un empleado le pregunta por qué no se le permite usar una memoria USB para llevar archivos desde la computadora

de su casa a la computadora de su oficina. ¿Cuál de las siguientes es la mejor respuesta?

R. Las memorias USB no tienen la capacidad de almacenar los datos necesarios.

B. Los datos de una memoria USB no se pueden cifrar.

C. Las memorias USB son demasiado grandes para llevarlas de un lugar a otro.

D. La unidad podría llevar un virus de casa a la oficina.

8. ¿Cuál de las siguientes opciones describe mejor un virus troyano?

A. Software malintencionado desencadenado por un evento, como una fecha específica.

B. Un virus que se disfraza de un programa legítimo pero en realidad abre un puerto en el sistema

C. Software malicioso que supervisa su actividad en Internet

D. Un virus que se autorreplica

9. Bob instaló una aplicación en diez computadoras en la oficina hace más de seis meses, y la aplicación funcionó como se esperaba. El 12 de febrero de este año, la aplicación eliminó una serie de archivos críticos del sistema. ¿Qué tipo de virus es este?

A. Virus troyano

B. Virus del gusano

C. Rootkit

D. Bomba lógica

10. Al realizar una evaluación de seguridad, observa que uno de los sistemas tiene un pequeño dispositivo conectado entre el teclado y la computadora. ¿Qué es este dispositivo?

A. Virus troyano

B. Rootkit

C. Keylogger

D. Bomba lógica

11. ¿Qué tipo de rootkit reemplaza un archivo de controlador del sistema operativo con la esperanza de ocultarse?

A. Rootkit a nivel de biblioteca

B. Rootkit a nivel de kernel

C. Rootkit a nivel de aplicación

D. Rootkit virtualizado

12. Un usuario inicia sesión con una cuenta de usuario normal y luego explota una vulnerabilidad en el sistema operativo para obtener acceso administrativo al sistema. ¿Qué tipo de ataque es este?

A. Diccionario

B. Fuerza bruta

C. Desbordamiento del búfer

D. Escalada de privilegios

13. ¿Cuál es el término para una colección de sistemas que un hacker compromete y luego utiliza para realizar ataques adicionales?

A. CompNet

B. HackNet

C. Botnet

D. SurfNet

14. Un usuario te llama para revisar su sistema porque está funcionando lentamente. Observa no solo que el sistema funciona lentamente, sino que el software de análisis de virus no responde cuando intenta realizar un análisis de virus. ¿Cuál de las siguientes opciones representa la mejor acción a seguir para ejecutar un análisis de virus?

A. Habilite el firewall.

B. Arranque desde un disco en vivo/USB.

C. Desactive la NIC.

D. Desactive el firewall.

Amenazas contra el hardware

15. Su gerente se acerca a usted y le dice que ha estado leyendo sobre el concepto de discos en vivo y cómo los piratas informáticos los están utilizando para eludir la seguridad del sistema. ¿Qué haría para ayudar a proteger sus sistemas de este tipo de amenaza?

A. Desactive el arranque desde un disco en vivo.

B. Extraiga la unidad óptica.

C. Establezca una contraseña administrativa segura.

D. Implementar una política de bloqueo de cuentas.

16. ¿Cuál de las siguientes opciones se considera un problema de seguridad válido con los dispositivos de almacenamiento conectado a la red (NAS)?

Un. El dispositivo NAS ejecuta el protocolo SMB.

B. Si el dispositivo NAS no está configurado correctamente, un compromiso de seguridad podría comprometer todos los datos del dispositivo.

C. El dispositivo NAS ejecuta el protocolo NFS.

D. El dispositivo NAS tiene una interfaz web para la configuración.

17. Su gerente ha leído que es posible en teléfonos más antiguos habilitados para Bluetooth que un pirata informático recupere todos los datos del teléfono. ¿Qué tipo de ataque es este?

A. Bluejacking

B. Fuerza bruta

C. Buffersnarfing

D. Bluesnarfing

Preguntas basadas en el rendimiento

18. Usando la exhibición, enumere la técnica de mitigación en la columna correcta.

	Mobile Device	Malicious Software
1. Screen lock		
2. Update definitions		
3. Device encryption		
4. Use antivirus/anti-malware software		
5. Remote wipe		
6. Monitor open ports		

19. Identifique el comando que usaría en un sistema Windows para ver todos los puertos de escucha en el sistema: ____

RESPUESTAS DE AUTOPRUEBA

Problemas de seguridad con vulnerabilidades

1. **B. La** exfiltración de datos es cuando alguien transfiere datos fuera de un sistema sin permiso. ☑ Puede deshabilitar los puertos USB del sistema para evitar que los dispositivos de almacenamiento portátiles se conecten al sistema o utilizar soluciones DLP para evitar la transferencia de información no autorizada.

   ☒ **A, C** y **D** son incorrectos. El uso de software antivirus, la habilitación del Firewall de Windows o la deshabilitación de servicios innecesarios no evitarán la filtración de datos.

2. **D**. Las soluciones de prevención de pérdida de datos (DLP) están diseñadas para evitar que alguien copie datos confidenciales o envíe información confidencial en un mensaje de correo electrónico. ☑

   ☒ **A, B** y **C** son incorrectos. La traducción de direcciones de red (NAT) es una tecnología que oculta un esquema de direcciones IP internas, el control de acceso a la red (NAC) es una tecnología que limita los dispositivos que pueden conectarse a la red y DES es un protocolo de cifrado antiguo que se considera cifrado débil.

3. **C**. Cuando se encuentran nuevas vulnerabilidades con el software que su empresa está utilizando, debe aplicar los parches de seguridad lo antes posible para eliminar las vulnerabilidades. ☑

   ☒ **A, B** y **D** son incorrectos. Aunque debe seguir los procedimientos recomendados de usar HTTPS en lugar de HTTP, bloquear permisos en el sistema y usar un firewall basado en host, estos no están directamente relacionados con el riesgo de la vulnerabilidad que se encontró y no quitan la vulnerabilidad.

Identificación de amenazas físicas

4. **B**. Cuando se trata de la seguridad de los dispositivos móviles, es importante educar a los empleados sobre cómo borrar un dispositivo de forma remota o informar el dispositivo perdido de inmediato para que el administrador de red pueda borrarlo de forma remota. ☑

   ☒ **A, C** y **D** son incorrectos. Aunque su gerente de ventas puede terminar solicitando un dispositivo de reemplazo a la gerencia, lo primero que debe hacer es borrar los datos del dispositivo borrándolo de forma remota o pidiéndole a un administrador que lo borre de forma remota. Podría intentar llamar al teléfono y pedir que se lo devuelvan, pero desde el punto de vista de la seguridad, el dispositivo debe borrarse como primer paso. Deshabilitar Bluetooth no es una opción válida, porque ella no está en posesión del dispositivo.

5. **C**. Todos los documentos confidenciales deben enviarse a través de una trituradora antes de desechar el papel. ☑

   ☒ **A, B** y **D** son incorrectos. Estas acciones no protegen la información confidencial de caer en manos de otras personas.

6. **A**. Para proteger los equipos informáticos pequeños, como pantallas LCD, proyectores y computadoras portátiles, de ser robados fácilmente, use un cable de bloqueo para asegurar el equipo a un escritorio. ☑

   ☒ **B, C** y **D** son incorrectos. En este ejemplo, está buscando un control de seguridad físico, como un cable de bloqueo. Aunque el cifrado de la unidad y la desactivación del arranque desde un disco en vivo son excelentes pasos para mejorar la seguridad, no evitarán que alguien robe el dispositivo. Estas opciones pueden proteger los datos en el dispositivo, pero no evitarán que el dispositivo sea robado. Cerrar la sesión de una estación no protegerá el sistema en absoluto sin seguridad física.

Mirando el software malicioso

7. **D**. Una de las principales preocupaciones con el uso de la memoria USB es el hecho de que un virus gusano puede replicarse a la memoria USB, y luego la unidad podría conectarse a un sistema corporativo, permitiendo que el virus se propague por todo el sistema. ☑

   ☒ **A, B** y **C** son incorrectos. Las memorias USB tienen grandes capacidades, suficientes para almacenar los datos del usuario típico, y no son demasiado grandes para transportarlas. Los datos en una memoria USB pueden, y deben, cifrarse.

8. **B**. Un virus troyano es un virus que se disfraza de un programa legítimo y, cuando se instala, abre el sistema al pirata informático, normalmente abriendo un puerto en el sistema. ☑

   ☒ **A, C** y **D** son incorrectos. Una bomba lógica es un software malicioso que se activa por un evento como una fecha específica. El spyware es un software malicioso que supervisa su actividad en Internet, y un gusano es un virus que se autorreplica.

9. **D**. Una bomba lógica es un software malicioso que se activa por un evento como una fecha específica. ☑

   ☒ **A, B** y **C** son incorrectos. Un virus troyano es un virus que se disfraza de un programa legítimo y, cuando se instala, abre el sistema al pirata informático, normalmente abriendo un puerto en el sistema. Un virus gusano es un virus autorreplicante, y un rootkit es una puerta trasera plantada en un sistema que le da a un hacker acceso administrativo al sistema.

10. C. Un keylogger en este caso es un dispositivo de hardware conectado entre el teclado y la computadora y está diseñado para capturar las pulsaciones de teclas de un usuario. ☑

    ☒ **A, B** y **D** son incorrectos. Un virus troyano es un virus que se disfraza de un programa legítimo y, cuando se instala, abre el sistema al pirata informático, normalmente abriendo un puerto en el sistema. Un rootkit es una puerta trasera plantada en un sistema que le da a un hacker ac-

ceso administrativo al sistema. Una bomba lógica es un software malicioso que se activa por un evento como una fecha específica.

11. B. Un rootkit a nivel de kernel reemplaza los archivos centrales del sistema operativo, como un archivo de controlador, con la esperanza de ocultarse. ☑

☒ **A, C** y **D** son incorrectos. Un rootkit de nivel de biblioteca es una DLL que se reemplaza en el sistema, mientras que un rootkit de nivel de aplicación viene en forma de un archivo EXE y se planta en el sistema. Un rootkit virtualizado se carga tan pronto como se inicia una computadora y luego carga el sistema operativo real.

12. D. La escalada de privilegios es cuando alguien aumenta sus permisos o derechos del nivel de usuario al nivel administrativo. ☑ Esto se hace normalmente explotando el sistema operativo o el software que se ejecuta en el sistema operativo.

☒ **A, B** y **C** son incorrectos. Los ataques de diccionario y fuerza bruta son tipos de ataques de contraseña y no implican elevar el nivel de acceso de alguien a un sistema. Un desbordamiento de búfer es un tipo de ataque contra el software que ayuda en la escalada de privilegios.

13. C. Una botnet es una serie de sistemas de los que el hacker tiene control y utiliza en ataques como spam y ataques de denegación de servicio. ☑

☒ **A, B** y **D** son incorrectos. Estos no son términos relacionados con la seguridad.

14. B. Puede arrancar desde un disco en vivo / unidad USB que creó que ejecuta su propio sistema operativo y tiene software de protección contra virus o, según lo admitido por algún software antivirus, crear medios de arranque desde los que puede arrancar para invocar el escaneo. ☑ El punto clave aquí es que no puede confiar en el sistema operativo existente que se ejecuta en la computadora una vez que se ha visto comprometido.

☒ **A, C** y **D** son incorrectos. Estos no representan lo que debe hacer a continuación para invocar un análisis de virus.

Amenazas contra el hardware

15. **A.** ☑ Para mantener un alto nivel de seguridad en sus sistemas, deshabilite el arranque desde discos en vivo o incluso cambie el orden de arranque para que el disco duro siempre arranque antes que cualquier disco óptico.

☒ **B, C** y **D** son incorrectos. Quitar la unidad óptica no es una gran respuesta, ya que significa que el usuario no tendrá un dispositivo de disco óptico. Implementar una contraseña segura en la cuenta administrativa y tener una política de bloqueo de cuenta tampoco son buenas opciones, ya que se omitirán cuando se use un disco en vivo.

16. B. Si el dispositivo NAS es golpeado con un virus o es pirateado, entonces el incidente de seguridad puede aplicarse a todos los archivos de la empresa si todos los datos están almacenados en el dispositivo NAS. ☑ Se debe tener mucho cuidado con la configuración del dispositivo NAS.

☒ **A, C** y **D** son incorrectos. La mayoría de los dispositivos NAS ejecutan protocolos SMB y NFS para que los clientes se conecten a los datos y no se consideran problemas de seguridad. El dispositivo NAS también tiene un dispositivo de interfaz web que puede utilizar para realizar los cambios de configuración en el dispositivo.

17. D. Bluesnarfing es la explotación de dispositivos Bluetooth y la recuperación de datos de ellos. ☑

☒ **A, B** y **C** son incorrectos. Bluejacking es otro exploit popular contra dispositivos Bluetooth y es el envío de mensajes no solicitados a dispositivos Bluetooth. Las respuestas B y C no son términos de seguridad reales.

Preguntas basadas en el rendimiento

18. A continuación se identifica a qué columna pertenece cada técnica de mitigación. Tenga en cuenta que para preguntas similares, el examen Security+ puede pedirle que arrastre los elementos a sus columnas correspondientes.

Mobile Device	Malicious Software
1. Screen lock	2. Update definitions
3. Device encryption	4. Use antivirus/anti-malware software
5. Remote wipe	6. Monitor open ports

19. Identifique el comando que usaría en un sistema Windows para ver todos los puertos de escucha en el sistema: **netstat -na**