Publicación especial 800-115

National Institute of
Standards and Technology
U.S. Department of Commerce

Guía técnica para

Pruebas y evaluación de seguridad de la información

Recomendaciones del Instituto Nacional de Estándares y Tecnología

Karen Scarfone
Murugiah Souppaya
Amanda Cody
Ángela Orebaugh

Publicación especial 800-115 del NIST

Guía técnica sobre seguridad de la información
Pruebas y evaluación

Recomendaciones de la Asamblea Nacional
Instituto de Normas y Tecnología

Karen Scarfone
Murugiah Souppaya
Amanda Cody
Ángela Orebaugh

SEGURIDAD INFORMÁTICA

División de Seguridad Informática
Laboratorio de Tecnología de la Información
Instituto Nacional de Estándares y Tecnología
Gaithersburg, MD 20899-8930

Septiembre de 2008

Departamento de Comercio de los Estados Unidos

Carlos M. Gutiérrez, Secretario

Instituto Nacional de Estándares y Tecnología

Dr. Patrick D. Gallagher, Subdirector

Informes sobre tecnología de sistemas informáticos

El Laboratorio de Tecnologías de la Información (ITL) del Instituto Nacional de Estándares y Tecnología (NIST) impulsa la economía y el bienestar público de Estados Unidos al proporcionar liderazgo técnico para la infraestructura nacional de medición y estandarización. El ITL desarrolla pruebas, métodos de prueba, datos de referencia, implementaciones de prueba de concepto y análisis técnicos para promover el desarrollo y el uso productivo de las tecnologías de la información (TI). Entre sus responsabilidades se incluye el desarrollo de estándares y directrices técnicas, físicas, administrativas y de gestión para la seguridad y privacidad rentables de la información sensible no clasificada en los sistemas informáticos federales. Esta publicación especial de la serie 800 informa sobre las actividades de investigación, asesoramiento y divulgación del ITL en materia de seguridad informática, así como sobre sus colaboraciones con la industria, el gobierno y organizaciones académicas.

Publicación especial 800-115 del Instituto Nacional de Estándares y Tecnología, 80 páginas
(septiembre de 2008)

Expresiones de gratitud

Los autores, Karen Scarfone y Murugiah Souppaya del Instituto Nacional de Estándares y Tecnología (NIST), y Amanda Cody y Angela Orebaugh de Booz Allen Hamilton, desean agradecer a sus colegas que revisaron los borradores de este documento y contribuyeron a su contenido técnico. Los autores agradecen la valiosa y perspicaz ayuda de John Connor, Tim Grance, Blair Heiserman, Arnold Johnson, Richard Kissel, Ron Ross, Matt Scholl y Pat Toth del NIST, así como la de Steve Allison, Derrick Dicoi, Daniel Owens, Victoria Thompson, Selena Tonti, Theodore Winograd y Gregg Zepp de Booz Allen Hamilton durante la elaboración del documento. Los autores agradecen todos los comentarios recibidos durante el período de consulta pública, en especial los de Marshall Abrams, Karen Quigg y otros miembros de MITRE Corporation; William Mills de SphereCom Enterprises; y los representantes del Servicio de Gestión Financiera (Departamento del Tesoro) y del Departamento de Salud y Servicios Humanos (HHS).

Información sobre marcas comerciales

Tabla de contenido

Lista de apéndices

Lista de tablas

Lista de figuras

Resumen ejecutivo

Una evaluación de seguridad de la información es el proceso para determinar la eficacia con la que una entidad evaluada (por ejemplo, un host, sistema, red, procedimiento o persona, conocido como objeto de evaluación) cumple con objetivos de seguridad específicos. Para ello, se pueden utilizar tres métodos de evaluación: pruebas, análisis y entrevistas. Las pruebas consisten en someter uno o más objetos de evaluación a condiciones específicas para comparar su comportamiento real con el esperado. El análisis implica verificar, inspeccionar, revisar, observar, estudiar o analizar uno o más objetos de evaluación para facilitar la comprensión, obtener aclaraciones u obtener evidencia. Las entrevistas consisten en conversar con personas o grupos dentro de una organización para facilitar la comprensión, obtener aclaraciones o identificar la ubicación de la evidencia. Los resultados de la evaluación se utilizan para determinar la eficacia de los controles de seguridad a lo largo del tiempo.

Este documento sirve de guía para los aspectos técnicos básicos de la realización de evaluaciones de seguridad de la información. Presenta métodos y técnicas de pruebas y análisis que una organización puede utilizar como parte de una evaluación, y ofrece información valiosa a los evaluadores sobre su ejecución y el impacto potencial que pueden tener en los sistemas y las redes. Para que una evaluación sea exitosa y tenga un impacto positivo en la seguridad de un sistema (y, en última instancia, de toda la organización), es necesario que otros elementos, además de la ejecución de las pruebas y el análisis, respalden el proceso técnico. Esta guía también incluye sugerencias para estas actividades, como un proceso de planificación sólido, un análisis de la causa raíz y la elaboración de informes personalizados.

Los procesos y la guía técnica presentados en este documento permiten a las organizaciones:

- Desarrollar una política, metodología y roles y responsabilidades individuales para la evaluación de la seguridad de la información, relacionados con los aspectos técnicos de la evaluación.
- Planifique con precisión una evaluación técnica de seguridad de la información, proporcionando orientación sobre cómo determinar qué sistemas evaluar y el enfoque de la evaluación, abordando las consideraciones logísticas, desarrollando un plan de evaluación y asegurando que se tengan en cuenta las consideraciones legales y normativas.
- Realizar de forma segura y eficaz una evaluación técnica de seguridad de la información utilizando los métodos y técnicas presentados, y responder a cualquier incidente que pueda ocurrir durante la evaluación.
- Gestionar adecuadamente los datos técnicos (recopilación, almacenamiento, transmisión y destrucción) durante todo el proceso de evaluación.
- Realizar análisis e informes para traducir los hallazgos técnicos en acciones de mitigación de riesgos que mejoren la postura de seguridad de la organización.

La información presentada en esta publicación está destinada a ser utilizada para diversos fines de evaluación. Por ejemplo, algunas evaluaciones se centran en verificar que un control de seguridad específico (o varios) cumpla con los requisitos, mientras que otras tienen como objetivo identificar, validar y evaluar las vulnerabilidades de seguridad explotables de un sistema. Las evaluaciones también se realizan para mejorar la capacidad de una organización de mantener una defensa proactiva de su red informática. Cabe destacar que las evaluaciones no sustituyen la implementación de controles de seguridad ni el mantenimiento de la seguridad del sistema.

Para llevar a cabo evaluaciones de seguridad técnica y garantizar que las pruebas y los exámenes de seguridad técnica aporten el máximo valor, el NIST recomienda que las organizaciones:

- Establezca una política de evaluación de seguridad de la información. Esta política define los requisitos de la organización para la realización de evaluaciones y establece la responsabilidad de las mismas.

Es fundamental que las personas se aseguren de que las evaluaciones se realicen de acuerdo con estos requisitos. Una política de evaluación debe abordar temas como los requisitos organizacionales que deben cumplir las evaluaciones, las funciones y responsabilidades, la adhesión a una metodología de evaluación establecida, la frecuencia de las evaluaciones y los requisitos de documentación.

Implemente una metodología de evaluación repetible y documentada. Esto proporciona coherencia y estructura a las evaluaciones, agiliza la incorporación de nuevo personal evaluador y aborda las limitaciones de recursos asociadas a las mismas. El uso de dicha metodología permite a las organizaciones maximizar el valor de las evaluaciones y minimizar los posibles riesgos derivados de ciertas técnicas de evaluación técnica. Estos riesgos pueden abarcar desde la falta de información suficiente sobre la postura de seguridad de la organización por temor a afectar la funcionalidad del sistema, hasta la afectación de la disponibilidad del sistema o la red al ejecutar técnicas sin las debidas medidas de seguridad. Los procesos que minimizan el riesgo causado por ciertas técnicas de evaluación incluyen el uso de evaluadores capacitados, el desarrollo de planes de evaluación integrales, el registro de las actividades de los evaluadores, la realización de pruebas fuera del horario laboral y la realización de pruebas en réplicas de sistemas de producción (por ejemplo, sistemas de desarrollo). Las organizaciones deben determinar el nivel de riesgo que están dispuestas a aceptar para cada evaluación y adaptar sus enfoques en consecuencia.

Determine los objetivos de cada evaluación de seguridad y adapte el enfoque en consecuencia. Las evaluaciones de seguridad tienen objetivos específicos, niveles de riesgo aceptables y recursos disponibles. Dado que ninguna técnica individual proporciona una visión completa de la seguridad de una organización cuando se implementa por sí sola, las organizaciones deben utilizar una combinación de técnicas. Esto también ayuda a limitar el riesgo y el uso de recursos.

Analice los hallazgos y desarrolle técnicas de mitigación de riesgos para abordar las debilidades. Para garantizar que las evaluaciones de seguridad aporten su máximo valor, las organizaciones deben realizar un análisis de causa raíz al finalizar la evaluación, lo que permitirá traducir los hallazgos en técnicas de mitigación prácticas. Estos resultados pueden indicar que las organizaciones deben abordar no solo las debilidades técnicas, sino también las deficiencias en los procesos y procedimientos organizacionales.

1. Introducción

1.1 Autoridad

El Instituto Nacional de Estándares y Tecnología (NIST) desarrolló este documento en cumplimiento de sus responsabilidades legales bajo la Ley Federal de Gestión de Seguridad de la Información (FISMA) de 2002, Ley Pública 107-347.

El NIST es responsable de desarrollar normas y directrices, incluidos los requisitos mínimos, para garantizar la seguridad de la información adecuada para todas las operaciones y activos de las agencias; sin embargo, dichas normas y directrices no se aplicarán a los sistemas de seguridad nacional. Esta directriz es coherente con los requisitos de la Circular A-130 de la Oficina de Administración y Presupuesto (OMB), Sección 8b (3), «Protección de los sistemas de información de las agencias», según se analiza en el Apéndice IV de la A-130: Análisis de las secciones clave. Se proporciona información complementaria en el Apéndice III de la A-130.

Esta guía se ha elaborado para uso de las agencias federales. Las organizaciones no gubernamentales pueden utilizarla de forma voluntaria y no está sujeta a derechos de autor, aunque se agradece que se cite la fuente.

Nada de lo dispuesto en este documento debe interpretarse como una contradicción con las normas y directrices que el Secretario de Comercio ha hecho obligatorias y vinculantes para las agencias federales en virtud de la autoridad legal; ni deben interpretarse estas directrices como una alteración o sustitución de las facultades existentes del Secretario de Comercio, del Director de la OMB o de cualquier otro funcionario federal.

1.2 Propósito y alcance

El propósito de este documento es brindar directrices a las organizaciones para la planificación y realización de pruebas y evaluaciones técnicas de seguridad de la información, el análisis de los resultados y el desarrollo de estrategias de mitigación. Ofrece recomendaciones prácticas para el diseño, la implementación y el mantenimiento de la información técnica relativa a los procesos y procedimientos de pruebas y evaluaciones de seguridad, que pueden utilizarse para diversos fines, como la detección de vulnerabilidades en un sistema o red y la verificación del cumplimiento de una política u otros requisitos. Esta guía no pretende presentar un programa integral de pruebas o evaluaciones de seguridad de la información, sino más bien una visión general de los elementos clave de las pruebas y evaluaciones técnicas de seguridad, con énfasis en técnicas específicas, sus ventajas y limitaciones, y recomendaciones para su uso.

Este documento reemplaza la publicación especial 800-42 del NIST, Guía sobre pruebas de seguridad de redes.

1.3 Audiencia

Esta guía está dirigida al personal de seguridad informática, a los responsables de programas, a los administradores de sistemas y redes, y a otro personal técnico encargado de los aspectos técnicos de la preparación, el funcionamiento y la seguridad de sistemas e infraestructuras de red. Los responsables también pueden utilizar la información presentada para facilitar la toma de decisiones técnicas relacionadas con las pruebas y evaluaciones de seguridad. El contenido de este documento es de carácter técnico y presupone que los lectores poseen al menos conocimientos básicos de seguridad de sistemas y redes.

1.4 Estructura del documento

El resto de este documento está organizado en siete secciones principales:

La sección 2 presenta una visión general de las evaluaciones de seguridad de la información, incluyendo políticas, roles y responsabilidades, metodologías y técnicas.

La sección 3 proporciona una descripción detallada de varias técnicas de examen técnico, incluyendo la revisión de documentación, la revisión de registros, el análisis de la red y la comprobación de la integridad de los archivos.

La sección 4 describe varias técnicas para identificar objetivos y analizarlos en busca de posibles vulnerabilidades. Algunos ejemplos de estas técnicas son el descubrimiento de redes y el escaneo de vulnerabilidades.

La sección 5 explica técnicas comúnmente utilizadas para validar la existencia de vulnerabilidades, como el descifrado de contraseñas y las pruebas de penetración.

La sección 6 presenta un enfoque y un proceso para planificar una evaluación de seguridad.

La sección 7 analiza los factores clave para la realización de evaluaciones de seguridad, incluyendo la coordinación, la evaluación en sí misma, el análisis y el manejo de datos.

La sección 8 presenta un enfoque para informar los resultados de la evaluación y proporciona una descripción general de las actividades de remediación.

Esta guía también contiene los siguientes apéndices:

El Apéndice A describe dos distribuciones de CD de sistemas operativos (SO) en vivo que permiten al usuario arrancar un ordenador desde un CD que contiene un SO totalmente operativo y herramientas de prueba.

El Apéndice B proporciona una plantilla para crear Reglas de Compromiso (ROE).

El Apéndice C analiza brevemente la evaluación de la seguridad de las aplicaciones.

El Apéndice D contiene recomendaciones para realizar pruebas de acceso remoto.

El Apéndice E ofrece una lista de recursos que pueden facilitar el proceso de evaluación de seguridad.

El Apéndice F incluye un glosario de términos utilizados a lo largo de este documento.

El Apéndice G proporciona una lista de acrónimos y abreviaturas.

2. Descripción general de las pruebas y exámenes de seguridad

Una evaluación de seguridad de la información es el proceso para determinar la eficacia con la que una entidad evaluada (por ejemplo, un host, sistema, red, procedimiento o persona, conocido como objeto de evaluación) cumple con objetivos de seguridad específicos. Para ello, se pueden utilizar tres métodos de evaluación: pruebas, análisis y entrevistas. Las pruebas consisten en someter uno o más objetos de evaluación a condiciones específicas para comparar su comportamiento real con el esperado. El análisis implica verificar, inspeccionar, revisar, observar, estudiar o analizar uno o más objetos de evaluación para facilitar la comprensión, obtener aclaraciones u obtener evidencia. Las entrevistas consisten en conversar con personas o grupos dentro de una organización para facilitar la comprensión, obtener aclaraciones o identificar la ubicación de la evidencia. Los resultados de la evaluación se utilizan para determinar la eficacia de los controles de seguridad a lo largo del tiempo.

Esta publicación aborda las técnicas de prueba y examen técnico que pueden utilizarse para identificar, validar y evaluar vulnerabilidades técnicas, y ayudar a las organizaciones a comprender y mejorar la seguridad de sus sistemas y redes. Las pruebas y el examen de seguridad son un requisito de FISMA1.
y otras normativas. No pretende sustituir la implementación de controles de seguridad ni el mantenimiento de la seguridad del sistema, sino ayudar a las organizaciones a confirmar que sus sistemas están debidamente protegidos e identificar cualquier requisito de seguridad que no se cumpla, así como otras vulnerabilidades que deban abordarse.

Esta sección ofrece una visión general de las metodologías de evaluación de la seguridad de la información y de las técnicas de prueba y examen técnico.

2.1 Metodología de evaluación de la seguridad de la información

Una metodología de evaluación de seguridad repetible y documentada resulta beneficiosa ya que puede:

- Proporcionar coherencia y estructura a las pruebas de seguridad puede minimizar los riesgos asociados.
- Agilizar la transición del nuevo personal de evaluación
- Abordar las limitaciones de recursos asociadas a las evaluaciones de seguridad.

Dado que la evaluación de la seguridad de la información requiere recursos como tiempo, personal, hardware y software, la disponibilidad de recursos suele ser un factor limitante en el tipo y la frecuencia de las evaluaciones de seguridad.
Evaluar los tipos de pruebas y exámenes de seguridad que la organización llevará a cabo, desarrollar una metodología apropiada, identificar los recursos necesarios y estructurar el proceso de evaluación para que cumpla con los requisitos previstos puede mitigar el desafío de los recursos. Esto permite a la organización reutilizar recursos ya existentes, como personal capacitado y plataformas de prueba estandarizadas; reduce el tiempo necesario para realizar la evaluación y la necesidad de adquirir equipos y software de prueba; y disminuye los costos generales de la evaluación.

Una metodología de evaluación de seguridad de la información por fases ofrece numerosas ventajas. Su estructura es fácil de seguir y proporciona puntos de inflexión naturales para la transición del personal. Dicha metodología debe contener, como mínimo, las siguientes fases:

[1] La sección 3544 exige la "prueba y evaluación periódicas de la eficacia de las políticas y procedimientos de seguridad de la información, y prácticas, que se realizarán con una frecuencia que dependerá del riesgo, pero no inferior a una vez al año." FISMA está disponible en http://csrc.nist.gov/drivers/documents/FISMA-final.pdf.

Planificación. Fundamental para una evaluación de seguridad exitosa, la fase de planificación se utiliza para recopilar la información necesaria para su ejecución, como los activos a evaluar, las amenazas que los afectan y los controles de seguridad que se utilizarán para mitigarlas, así como para desarrollar el enfoque de la evaluación. Una evaluación de seguridad debe tratarse como cualquier otro proyecto, con un plan de gestión que aborde las metas y los objetivos, el alcance, los requisitos, las funciones y responsabilidades del equipo, las limitaciones, los factores de éxito, las suposiciones, los recursos, el cronograma y los entregables. La sección 6 de esta guía trata sobre la planificación.

Ejecución. Los objetivos principales de la fase de ejecución son identificar vulnerabilidades y validarlas cuando corresponda. Esta fase debe abarcar las actividades relacionadas con el método y la técnica de evaluación previstos. Si bien las actividades específicas de esta fase varían según el tipo de evaluación, al finalizarla, los evaluadores habrán identificado vulnerabilidades en el sistema, la red y los procesos organizacionales. Esta fase se analiza con mayor detalle en la Sección 7.

Fase posterior a la ejecución. Esta fase se centra en analizar las vulnerabilidades identificadas para determinar las causas raíz, establecer recomendaciones de mitigación y elaborar un informe final. La sección 8 de esta guía trata sobre la elaboración de informes y la mitigación.

Existen diversas metodologías aceptadas para realizar diferentes tipos de evaluaciones de seguridad de la información. En el Apéndice E.2 se incluyen referencias a varias de estas metodologías. Por ejemplo, el NIST ha creado una metodología —documentada en la Publicación Especial (SP) 800-53A, Guía para la Evaluación de los Controles de Seguridad en los Sistemas de Información Federales— que ofrece sugerencias para evaluar la eficacia de los controles de seguridad descritos en la NIST SP 800-53.3 Otra metodología de evaluación ampliamente utilizada es el Manual de Metodología de Pruebas de Seguridad de Código Abierto (OSSTMM).4 Dado que existen numerosas razones para realizar evaluaciones, una organización podría optar por utilizar varias metodologías. Esta publicación ofrece recomendaciones sobre técnicas de prueba y examen que pueden emplearse con diversas metodologías de evaluación y aprovecharse para múltiples propósitos.

2.2 Técnicas de evaluación técnica

Existen docenas de técnicas de prueba y análisis de seguridad técnica que pueden utilizarse para evaluar el nivel de seguridad de sistemas y redes. Las técnicas más utilizadas, desde la perspectiva de este documento, se analizarán con mayor detalle más adelante en esta guía y se agrupan en las siguientes tres categorías:

Técnicas de revisión. Estas técnicas de examen se utilizan para evaluar sistemas, aplicaciones, redes, políticas y procedimientos con el fin de descubrir vulnerabilidades, y generalmente se realizan de forma manual. Incluyen la revisión de documentación, registros, conjuntos de reglas y configuración del sistema; el análisis del tráfico de red; y la comprobación de la integridad de los archivos. La sección 3 proporciona información adicional sobre las técnicas de revisión.

Técnicas de identificación y análisis de objetivos. Estas técnicas de prueba permiten identificar sistemas, puertos, servicios y posibles vulnerabilidades, y aunque pueden realizarse manualmente, generalmente se llevan a cabo mediante herramientas automatizadas. Incluyen el descubrimiento de redes, puertos de red y servicios.

---

2 NIST no respalda una metodología sobre otra; la intención es brindar a las organizaciones opciones que les permitan tomar decisiones informadas para adoptar una metodología existente o combinar varias para desarrollar una metodología única que se adapte a la organización.

3 La publicación especial 800-53A del NIST (NIST SP 800-53A) aborda el marco para el desarrollo de procedimientos de evaluación, describe el proceso de evaluación de los controles de seguridad y ofrece procedimientos de evaluación para cada control. Esta publicación se desarrolló para usarse junto con la publicación especial 800-37 del NIST (NIST SP 800-37), Guía para la Certificación y Acreditación de Seguridad de los Sistemas de Información Federales. Los NIST SP 800-53, 800-53A y 800-37 están disponibles en http://csrc.nist.gov/publications/PubsSPs.html.

4 Puede encontrar más información sobre OSSTMM en http://www.isecom.org/osstmm/.

Identificación, escaneo de vulnerabilidades, escaneo inalámbrico y examen de seguridad de aplicaciones. En la sección 4 se presenta una discusión más detallada de estas técnicas.

Técnicas de validación de vulnerabilidades. Estas técnicas de prueba corroboran la existencia de vulnerabilidades y pueden realizarse manualmente o mediante herramientas automáticas, según la técnica específica empleada y la experiencia del equipo de pruebas. Entre las técnicas de validación de vulnerabilidades se incluyen el descifrado de contraseñas, las pruebas de penetración, la ingeniería social y las pruebas de seguridad de aplicaciones. En la sección 5 encontrará más información sobre estas técnicas.

Dado que ninguna técnica por sí sola puede ofrecer una visión completa de la seguridad de un sistema o red, las organizaciones deben combinar las técnicas adecuadas para garantizar evaluaciones de seguridad sólidas. Por ejemplo, las pruebas de penetración suelen basarse en la identificación de puertos y servicios de red, así como en el escaneo de vulnerabilidades para identificar hosts y servicios que podrían ser objetivos de futuros ataques. Asimismo, existen diversas técnicas para cumplir con los requisitos de una evaluación, como determinar si los parches se han aplicado correctamente. Esta publicación se centra en explicar cómo se pueden realizar estas diferentes técnicas, sin especificar cuáles deben utilizarse en cada circunstancia, lo que brinda a las organizaciones la flexibilidad de elegir las que mejor se adapten a sus necesidades.

Además de las técnicas técnicas descritas en esta publicación, existen numerosas técnicas no técnicas que pueden utilizarse de forma complementaria o sustitutiva de las técnicas técnicas. Un ejemplo son las pruebas de seguridad física, que confirman la existencia de vulnerabilidades de seguridad física al intentar eludir cerraduras, lectores de tarjetas y otros controles de seguridad física, generalmente para obtener acceso no autorizado a equipos específicos. Otro ejemplo de técnica no técnica es la identificación manual de activos. Una organización puede optar por identificar los activos que se van a evaluar mediante inventarios de activos, recorridos físicos por las instalaciones y otros medios no técnicos, en lugar de recurrir a técnicas técnicas para la identificación de activos. Los detalles sobre las técnicas no técnicas no se incluyen en esta publicación, pero es importante reconocer su valor y considerar cuándo pueden ser más apropiadas que sus contrapartes técnicas.

2.3 Comparación de pruebas y exámenes

Las evaluaciones consisten principalmente en la revisión de documentos como políticas, procedimientos, planes de seguridad, requisitos de seguridad, procedimientos operativos estándar, diagramas de arquitectura, documentación técnica, inventarios de activos, configuraciones del sistema, conjuntos de reglas y registros del sistema. Se realizan para determinar si un sistema está debidamente documentado y para obtener información sobre aspectos de seguridad que solo están disponibles a través de la documentación. Esta documentación identifica el diseño, la instalación, la configuración, el funcionamiento y el mantenimiento previstos de los sistemas y la red, y su revisión y comparación garantizan la conformidad y la coherencia. Por ejemplo, los requisitos de seguridad de un entorno deben guiar la documentación, como los planes de seguridad del sistema y los procedimientos operativos estándar; por lo tanto, los evaluadores deben asegurarse de que todos los planes, procedimientos, arquitecturas y configuraciones cumplan con los requisitos de seguridad establecidos y las políticas aplicables. Otro ejemplo es la revisión del conjunto de reglas de un firewall para garantizar su cumplimiento con las políticas de seguridad de la organización en relación con el uso de Internet, como el uso de mensajería instantánea, el intercambio de archivos entre pares (P2P) y otras actividades prohibidas.

Por lo general, los exámenes no tienen impacto en los sistemas o redes reales del entorno objetivo, salvo el acceso a la documentación, los registros o los conjuntos de reglas necesarios. Sin embargo, si se van a recuperar archivos de configuración o registros del sistema de un sistema determinado, como un enrutador o un cortafuegos, solo los administradores del sistema y

[5] Una técnica de prueba pasiva que puede afectar a las redes es el análisis de tráfico de red, que consiste en conectar un analizador de tráfico a un concentrador, un puerto de derivación o un puerto de expansión de la red. En algunos casos, el proceso de conexión requiere la reconfiguración de un dispositivo de red, lo que podría interrumpir las operaciones.

Este trabajo debe ser realizado por personas con una formación similar para garantizar que la configuración no se modifique o elimine inadvertidamente.

Las pruebas implican el trabajo práctico con sistemas y redes para identificar vulnerabilidades de seguridad, y pueden realizarse en toda la empresa o en sistemas seleccionados. El uso de técnicas de escaneo y penetración puede proporcionar información valiosa sobre vulnerabilidades potenciales y predecir la probabilidad de que un adversario o intruso pueda explotarlas. Las pruebas también permiten a las organizaciones medir el nivel de cumplimiento en áreas como la gestión de parches, la política de contraseñas y la gestión de la configuración.

Si bien las pruebas pueden ofrecer una visión más precisa del estado de seguridad de una organización que las inspecciones, son más intrusivas y pueden afectar a los sistemas o redes del entorno objetivo. El nivel de impacto potencial depende de las técnicas de prueba específicas que se utilicen, las cuales pueden interactuar con los sistemas y redes objetivo de diversas maneras, como el envío de paquetes de red normales para determinar qué puertos están abiertos y cerrados, o el envío de paquetes especialmente diseñados para detectar vulnerabilidades. Siempre que una prueba o un evaluador interactúa directamente con un sistema o red, existe la posibilidad de que se produzcan interrupciones inesperadas del sistema y otras denegaciones de servicio. Las organizaciones deben determinar sus niveles aceptables de intrusividad al decidir qué técnicas utilizar. Excluir las pruebas que se sabe que generan denegaciones de servicio y otras interrupciones puede ayudar a reducir estos impactos negativos.

Las pruebas no ofrecen una evaluación exhaustiva de la postura de seguridad de una organización y, a menudo, tienen un alcance limitado debido a las restricciones de recursos, especialmente en lo que respecta al tiempo. Los atacantes maliciosos, por otro lado, pueden disponer del tiempo que necesiten para explotar y penetrar un sistema o red. Asimismo, si bien las organizaciones tienden a evitar el uso de técnicas de prueba que afecten a los sistemas o redes, los atacantes no están sujetos a esta limitación y utilizan cualquier técnica que consideren necesaria. En consecuencia, es menos probable que las pruebas, en comparación con los análisis, identifiquen debilidades relacionadas con la política y la configuración de seguridad. En muchos casos, la combinación de técnicas de prueba y análisis puede proporcionar una visión más precisa de la seguridad.

2.4 Puntos de vista de prueba

Las pruebas pueden realizarse desde diversas perspectivas; por ejemplo, ¿con qué facilidad un atacante externo o un empleado malintencionado podría atacar con éxito un sistema? La sección 2.4.1 de esta guía compara las pruebas realizadas desde perspectivas externas e internas. La sección 2.4.2 aborda otro aspecto de las perspectivas: el conocimiento previo que los evaluadores tienen del objetivo o del entorno objetivo.

2.4.1 Externo e interno

Las pruebas de seguridad externas se realizan desde fuera del perímetro de seguridad de la organización. Esto permite visualizar el estado de seguridad del entorno tal como se ve fuera del perímetro —generalmente desde Internet— con el objetivo de detectar vulnerabilidades que podrían ser explotadas por un atacante externo.

Las pruebas externas suelen comenzar con técnicas de reconocimiento que buscan en los registros públicos, la información de los servidores del Sistema de Nombres de Dominio (DNS), las publicaciones en grupos de noticias y otra información disponible públicamente para recopilar datos (por ejemplo, nombres de sistemas, direcciones IP, sistemas operativos, contactos técnicos) que puedan ayudar al evaluador a identificar vulnerabilidades. A continuación, se inicia la enumeración mediante técnicas de detección y escaneo de redes para determinar los hosts externos y los servicios en escucha.
Dado que las defensas perimetrales, como cortafuegos, enrutadores y listas de control de acceso, suelen limitar el tipo de tráfico permitido en la red interna, los evaluadores a menudo emplean técnicas para eludir estas defensas, al igual que los atacantes externos. Dependiendo de los protocolos permitidos, los ataques iniciales generalmente se centran en protocolos de aplicación comunes y permitidos, como el Protocolo de Transferencia de Archivos (FTP), el Protocolo de Transferencia de Hipertexto (HTTP), el Protocolo Simple de Transferencia de Correo (SMTP) y el Protocolo de Oficina de Correos.

(POP). Los servidores con acceso externo se someten a pruebas para detectar vulnerabilidades que podrían permitir el acceso a servidores internos e información privada. Las pruebas de seguridad externas también se centran en descubrir vulnerabilidades en los métodos de acceso, como puntos de acceso inalámbricos, módems y portales a servidores internos.

Para las pruebas de seguridad interna, los evaluadores trabajan desde la red interna y asumen la identidad de un empleado de confianza o de un atacante que ha vulnerado las defensas perimetrales. Este tipo de pruebas puede revelar vulnerabilidades que podrían ser explotadas y demuestra el daño potencial que este tipo de atacante podría causar. Las pruebas de seguridad interna también se centran en la seguridad y la configuración del sistema, incluyendo la configuración de aplicaciones y servicios, la autenticación, el control de acceso y el fortalecimiento del sistema.

Los evaluadores que realizan pruebas internas suelen tener cierto nivel de acceso a la red, normalmente como usuarios generales, y se les proporciona información que tendrían los usuarios con privilegios similares. Este nivel de acceso temporal depende de los objetivos de la prueba y puede llegar hasta los privilegios de un administrador de sistemas o de red. Partiendo del nivel de acceso que se les ha concedido, los evaluadores intentan obtener acceso adicional a la red y a los sistemas mediante la escalada de privilegios; es decir, aumentando los privilegios de usuario a privilegios de administrador, o los privilegios de administrador de sistemas a privilegios de administrador de dominio.

Las pruebas internas no están tan limitadas como las externas, ya que se realizan tras las defensas perimetrales, aunque existan cortafuegos, enrutadores y conmutadores internos que puedan suponer limitaciones. Además de las técnicas de prueba, se pueden utilizar técnicas de análisis como el análisis del tráfico de red.

Si se van a realizar pruebas tanto internas como externas, normalmente se realizan primero las externas. Esto resulta especialmente beneficioso si los mismos evaluadores van a realizar ambos tipos de pruebas, ya que evita que adquieran información privilegiada sobre la arquitectura de la red o la configuración del sistema que no estaría al alcance de un adversario, una ventaja que reduciría la validez de la prueba.

2.4.2 Manifiesto y Encubierto

Las pruebas de seguridad abiertas, también conocidas como pruebas de sombrero blanco, implican la realización de pruebas externas o internas con el conocimiento y consentimiento del personal de TI de la organización, lo que permite una evaluación integral de la seguridad de la red o el sistema. Dado que el personal de TI está plenamente informado y participa en las pruebas, puede ofrecer orientación para limitar su impacto. Las pruebas también pueden brindar una oportunidad de capacitación, ya que el personal observa las actividades y los métodos que utilizan los evaluadores para evaluar y, potencialmente, eludir las medidas de seguridad implementadas. Esto proporciona contexto a los requisitos de seguridad implementados o mantenidos por el personal de TI y, además, puede ayudar a enseñarles cómo realizar las pruebas.

Las pruebas de seguridad encubiertas, también conocidas como pruebas de sombrero negro, adoptan un enfoque adversarial al realizarse sin el conocimiento del personal de TI de la organización, pero con el pleno conocimiento y autorización de la alta dirección. Algunas organizaciones designan a un tercero de confianza para garantizar que la organización objetivo no inicie medidas de respuesta asociadas con el ataque sin antes verificar que este se esté produciendo (por ejemplo, que la actividad detectada no provenga de una prueba). En tales situaciones, el tercero de confianza actúa como intermediario para los evaluadores, la dirección, el personal de TI y el personal de seguridad, facilitando las actividades y la comunicación. Este tipo de prueba es útil para evaluar los controles de seguridad técnicos, la respuesta del personal de TI ante incidentes de seguridad percibidos y el conocimiento e implementación de la política de seguridad de la organización por parte del personal. Las pruebas encubiertas pueden realizarse con o sin previo aviso.

El objetivo de las pruebas encubiertas es examinar el daño o el impacto que un adversario puede causar; no se centra en identificar vulnerabilidades. Este tipo de pruebas no evalúa todos los controles de seguridad, ni identifica todas las vulnerabilidades, ni analiza todos los sistemas de una organización. Las pruebas encubiertas examinan la organización desde una perspectiva integral.

Desde una perspectiva adversaria, este tipo de prueba suele identificar y explotar las vulnerabilidades más básicas para obtener acceso a la red. Si el objetivo de una organización es emular a un adversario específico, este tipo de prueba requiere consideraciones especiales, como la adquisición y el modelado de datos de amenazas. Los escenarios resultantes ofrecen una visión estratégica general de los posibles métodos de explotación, el riesgo y el impacto de una intrusión. Las pruebas encubiertas suelen tener límites definidos, como detenerlas cuando se alcanza cierto nivel de acceso o cuando se puede provocar un determinado tipo de daño como siguiente paso en la prueba. Establecer estos límites previene daños, pero a la vez demuestra que estos podrían ocurrir.

Además de no detectar muchas vulnerabilidades, las pruebas encubiertas suelen ser costosas y consumir mucho tiempo debido a la necesidad de sigilo. Para operar en un entorno encubierto, un equipo de pruebas debe ralentizar sus escaneos y otras acciones para no ser detectado por el personal de seguridad de la organización objetivo. Cuando las pruebas se realizan internamente, también debe considerarse la capacitación en términos de tiempo y presupuesto. Asimismo, una organización puede tener personal capacitado para realizar actividades rutinarias como escaneos y evaluaciones de vulnerabilidades, pero no para técnicas especializadas como pruebas de penetración o de seguridad de aplicaciones. Las pruebas abiertas son menos costosas, conllevan menos riesgos que las encubiertas y se utilizan con mayor frecuencia; sin embargo, las pruebas encubiertas ofrecen una mejor indicación de la seguridad diaria de la organización objetivo, ya que los administradores de sistemas no estarán tan alerta.

3. Técnicas de revisión

Las técnicas de revisión examinan de forma pasiva sistemas, aplicaciones, redes, políticas y procedimientos para descubrir vulnerabilidades de seguridad. También recopilan información para facilitar y optimizar otras técnicas de evaluación. Debido a su naturaleza pasiva, las técnicas de revisión representan un riesgo mínimo para los sistemas y las redes. Esta sección abarca varias técnicas de revisión comunes: revisión de documentación, registros, conjuntos de reglas y configuración del sistema; análisis de tráfico de red; y verificación de la integridad de los archivos.

3.1 Revisión de la documentación

La revisión de la documentación determina si los aspectos técnicos de las políticas y los procedimientos están actualizados y son completos. Estos documentos constituyen la base de la postura de seguridad de una organización, pero a menudo se pasan por alto durante las evaluaciones técnicas. Los grupos de seguridad dentro de la organización deben proporcionar a los evaluadores la documentación pertinente para garantizar una revisión exhaustiva. Los documentos que se deben revisar para verificar su precisión técnica e integridad incluyen: políticas, arquitecturas y requisitos de seguridad; procedimientos operativos estándar; planes de seguridad del sistema y acuerdos de autorización; memorandos de entendimiento y acuerdos para las interconexiones del sistema; y planes de respuesta ante incidentes.

La revisión de la documentación puede detectar deficiencias y debilidades que podrían resultar en controles de seguridad faltantes o implementados incorrectamente. Los evaluadores suelen verificar que la documentación de la organización cumpla con estándares y regulaciones como FISMA, y buscan políticas deficientes o desactualizadas. Entre las debilidades comunes de la documentación se incluyen procedimientos o protocolos de seguridad del sistema operativo que ya no se utilizan, y la omisión de un nuevo sistema operativo y sus protocolos. La revisión de la documentación no garantiza que los controles de seguridad se implementen correctamente; solo verifica que existan las directrices y la orientación necesarias para respaldar la infraestructura de seguridad.

Los resultados de la revisión de la documentación pueden utilizarse para perfeccionar otras técnicas de prueba y análisis. Por ejemplo, si una política de gestión de contraseñas establece requisitos específicos en cuanto a la longitud y complejidad mínimas de las contraseñas, esta información puede utilizarse para configurar las herramientas de descifrado de contraseñas y lograr un rendimiento más eficiente.

3.2 Revisión de registros

La revisión de registros determina si los controles de seguridad registran la información correcta y si la organización cumple con sus políticas de gestión de registros. Como fuente de información histórica, los registros de auditoría pueden utilizarse para validar que el sistema opera de acuerdo con las políticas establecidas. Por ejemplo, si la política de registro establece que todos los intentos de autenticación a servidores críticos deben registrarse, la revisión de registros determinará si esta información se está recopilando y muestra el nivel de detalle adecuado. La revisión de registros también puede revelar problemas como servicios y controles de seguridad mal configurados, accesos no autorizados e intentos de intrusión. Por ejemplo, si un sensor de un sistema de detección de intrusiones (IDS) se encuentra detrás de un firewall, sus registros pueden utilizarse para examinar las comunicaciones que el firewall permite en la red. Si el sensor registra actividades que deberían bloquearse, indica que el firewall no está configurado de forma segura.

---

[6] Esta publicación aborda las revisiones desde la perspectiva de la evaluación. También se recomienda realizar revisiones periódicas como parte del monitoreo y mantenimiento regulares del sistema, por ejemplo, para identificar problemas operativos, configuraciones de seguridad erróneas, actividades maliciosas y otros tipos de incidentes de seguridad. Las organizaciones pueden optar por utilizar los resultados de las revisiones operativas para sus evaluaciones.

[7] La publicación especial 800-92 del NIST, « Guía para la gestión de registros de seguridad», proporciona más información sobre métodos y técnicas de gestión de registros de seguridad, incluida la revisión de registros. Está disponible en http://csrc.nist.gov/publications/PubsSPs.html.

Ejemplos de información de registro que pueden resultar útiles al realizar evaluaciones de seguridad técnica incluyen:

Los registros del servidor de autenticación o del sistema pueden incluir intentos de autenticación exitosos y fallidos.

Los registros del sistema pueden incluir información sobre el inicio y el cierre del sistema y los servicios, la instalación de software no autorizado, los accesos a archivos, los cambios en la política de seguridad, los cambios en las cuentas (por ejemplo, la creación y eliminación de cuentas, la asignación de privilegios de cuenta) y el uso de privilegios.

Los registros del sistema de detección y prevención de intrusiones pueden incluir actividad maliciosa e inapropiada.
usar.

Los registros del firewall y del enrutador pueden incluir conexiones salientes que indican dispositivos internos comprometidos (por ejemplo, rootkits, bots, troyanos, spyware).

Los registros del cortafuegos pueden incluir intentos de conexión no autorizados y uso inapropiado.

Los registros de la aplicación pueden incluir intentos de conexión no autorizados, cambios de cuenta, uso de privilegios e información sobre el uso de la aplicación o la base de datos.

Los registros del antivirus pueden incluir fallos de actualización y otros indicios de firmas y software obsoletos.

Los registros de seguridad, en particular la gestión de parches y algunos productos de sistemas de detección de intrusiones (IDS) y de prevención de intrusiones (IPS), pueden registrar información sobre servicios y aplicaciones vulnerables conocidos.

Revisar manualmente los registros puede ser extremadamente lento y engorroso. Existen herramientas de auditoría automatizadas que reducen significativamente el tiempo de revisión y generan informes predefinidos y personalizados que resumen el contenido de los registros y los vinculan a un conjunto de actividades específicas. Los evaluadores también pueden usar estas herramientas automatizadas para facilitar el análisis de registros, convirtiéndolos de diferentes formatos a un formato estándar. Además, si los evaluadores revisan una acción específica, como el número de intentos de inicio de sesión fallidos en una organización, pueden usar estas herramientas para filtrar los registros según la actividad que se esté comprobando.

3.3 Revisión del conjunto de reglas

Un conjunto de reglas es una colección de reglas o firmas con las que se compara el tráfico de red o la actividad del sistema para determinar qué acción tomar; por ejemplo, reenviar o rechazar un paquete, generar una alerta o permitir un evento del sistema. La revisión de estos conjuntos de reglas se realiza para garantizar su exhaustividad e identificar deficiencias y vulnerabilidades en los dispositivos de seguridad y en las defensas por capas, como vulnerabilidades de la red, infracciones de políticas y rutas de comunicación no deseadas o vulnerables. Una revisión también puede revelar ineficiencias que afectan negativamente al rendimiento de un conjunto de reglas.

Los conjuntos de reglas que se deben revisar incluyen los conjuntos de reglas de firewall de red y de host, los conjuntos de reglas de IDS/IPS y las listas de control de acceso de los enrutadores. La siguiente lista proporciona ejemplos de los tipos de comprobaciones que se realizan con mayor frecuencia en las revisiones de conjuntos de reglas:

Para listas de control de acceso de enrutadores

– Cada regla sigue siendo obligatoria (por ejemplo, las reglas que se añadieron con fines temporales son
(se eliminan tan pronto como ya no son necesarios)

Solo se permite el tráfico autorizado según la política; el resto se deniega por defecto.

Para conjuntos de reglas de firewall

– Cada regla sigue siendo obligatoria

Las reglas imponen el acceso con privilegios mínimos, como especificar únicamente las direcciones IP y los puertos necesarios.

– Las reglas más específicas se aplican antes que las reglas generales.

No hay puertos abiertos innecesarios que puedan cerrarse para reforzar la seguridad perimetral.

– El conjunto de reglas no permite que el tráfico eluda otras defensas de seguridad.

– En el caso de los conjuntos de reglas de firewall basados en host, las reglas no indican la presencia de puertas traseras, actividad de spyware ni aplicaciones prohibidas, como programas de intercambio de archivos entre pares.

Para conjuntos de reglas IDS/IPS

– Se han desactivado o eliminado las firmas innecesarias para eliminar los falsos positivos y mejorar el rendimiento

– Las firmas necesarias están habilitadas, se han ajustado correctamente y se mantienen adecuadamente.

3.4 Revisión de la configuración del sistema

La revisión de la configuración del sistema es el proceso de identificar vulnerabilidades en los controles de seguridad, como sistemas que no están reforzados o configurados según las políticas de seguridad. Por ejemplo, este tipo de revisión revelará servicios y aplicaciones innecesarios, configuraciones incorrectas de cuentas de usuario y contraseñas, y configuraciones inadecuadas de registro y copias de seguridad. Algunos ejemplos de archivos de configuración de seguridad que se pueden revisar son las políticas de seguridad de Windows y los archivos de configuración de seguridad de Unix, como los que se encuentran en /etc.

Los evaluadores que utilizan técnicas de revisión manual se basan en guías o listas de verificación de configuración de seguridad para comprobar que la configuración del sistema minimiza los riesgos de seguridad. Para realizar una revisión manual de la configuración del sistema, los evaluadores acceden a diversas opciones de seguridad del dispositivo evaluado y las comparan con las configuraciones recomendadas en la lista de verificación. Las configuraciones que no cumplen con los estándares mínimos de seguridad se marcan y se reportan.

El Protocolo de Automatización de Contenido de Seguridad (SCAP) es un método que utiliza estándares específicos para permitir la gestión automatizada de vulnerabilidades, su medición y la evaluación del cumplimiento de las políticas. Los archivos NIST SCAP están diseñados para el cumplimiento de FISMA y las pruebas de control de seguridad NIST SP 800-53A. Se pueden utilizar otras herramientas para recuperar e informar sobre la configuración de seguridad y proporcionar orientación para su corrección. Las herramientas automatizadas suelen ejecutarse directamente en el dispositivo que se está evaluando, pero también pueden ejecutarse en un sistema con acceso de red al dispositivo. Si bien las revisiones automatizadas de la configuración del sistema son más rápidas que los métodos manuales, es posible que aún existan configuraciones que deban revisarse manualmente. Tanto los métodos manuales como los automatizados requieren privilegios de administrador o de superusuario para ver la configuración de seguridad seleccionada.

En general, es preferible utilizar controles automatizados en lugar de controles manuales siempre que sea posible. Las comprobaciones automatizadas se pueden realizar muy rápidamente y proporcionan resultados consistentes y repetibles. Que una persona revise manualmente cientos o miles de configuraciones es tedioso y propenso a errores.

[8] NIST mantiene un repositorio de listas de verificación de configuración de seguridad para productos de TI en http://checklists.nist.gov/.

[9] Puede encontrar más información sobre SCAP en http://scap.nist.gov/.

3.5 Análisis de red

El análisis de tráfico de red es una técnica pasiva[1] que monitoriza la comunicación de la red, decodifica protocolos y examina cabeceras y cargas útiles para detectar información de interés. Además de utilizarse como técnica de revisión, el análisis de tráfico de red también puede emplearse para la identificación y el análisis de objetivos (véase la sección 4.1).

Entre los motivos para utilizar la interceptación de tráfico de red se incluyen los siguientes:

- Captura y reproducción del tráfico de red
- Realizar el descubrimiento pasivo de la red (por ejemplo, identificar los dispositivos activos en la red).
- Identificación de sistemas operativos, aplicaciones, servicios y protocolos, incluyendo protocolos no seguros (por ejemplo, telnet) y no autorizados (por ejemplo, intercambio de archivos entre pares).
- Identificar actividades no autorizadas e inapropiadas, como la transmisión no cifrada de información confidencial.
- Recopilar información, como nombres de usuario y contraseñas no cifrados.

La interceptación de tráfico de red tiene poco impacto en los sistemas y redes, siendo el impacto más notable en el uso del ancho de banda o la potencia de cómputo. El analizador de tráfico —la herramienta utilizada para realizar la interceptación de tráfico de red— Se requiere un medio para conectarse a la red, como un concentrador, un adaptador o un conmutador con capacidad de expansión de puertos. La expansión de puertos consiste en copiar el tráfico transmitido por todos los demás puertos al puerto donde está instalado el analizador de red. Las organizaciones pueden implementar analizadores de red en diversas ubicaciones dentro de un entorno. Estos suelen incluir lo siguiente:

- En el perímetro, para evaluar el tráfico que entra y sale de la red.
- Detrás de los cortafuegos, para evaluar que los conjuntos de reglas filtran correctamente el tráfico
- Detrás de los sistemas IDS/IPS, para determinar si las firmas se están activando y recibiendo la respuesta adecuada.
- Frente a un sistema o aplicación crítica para evaluar la actividad
- En un segmento de red específico, para validar protocolos cifrados.

Una limitación del análisis de tráfico de red es el uso de cifrado. Muchos atacantes se aprovechan del cifrado para ocultar sus actividades; si bien los analistas pueden ver que existe comunicación, no pueden acceder a su contenido. Otra limitación es que un analizador de tráfico de red solo puede analizar el tráfico del segmento local donde está instalado. Esto obliga al analista a trasladarlo de un segmento a otro, instalar varios analizadores en toda la red o utilizar técnicas de expansión de puertos. Además, a los analistas les puede resultar difícil localizar un puerto de red físico abierto para el análisis en cada segmento. Por otra parte, el análisis de tráfico de red es una actividad bastante laboriosa que requiere un alto grado de intervención humana para interpretar el tráfico de red.

3.6 Comprobación de la integridad de los archivos

Los verificadores de integridad de archivos permiten identificar si se han modificado archivos del sistema, calculando y almacenando una suma de comprobación para cada archivo protegido y creando una base de datos de sumas de comprobación. Las sumas de comprobación almacenadas se recalculan posteriormente para comparar su valor actual con el valor almacenado, lo que identifica el archivo.

---

[10] Los analizadores de red pueden realizar búsquedas de nombres de dominio para el tráfico que recopilan, generando así tráfico de red. Las búsquedas de nombres de dominio se pueden desactivar para un análisis de red sigiloso.

modificaciones. La capacidad de comprobación de la integridad de los archivos suele estar incluida en cualquier IDS comercial basado en host y también está disponible como una utilidad independiente.

Aunque un verificador de integridad no requiere mucha interacción humana, debe usarse con cuidado para garantizar su eficacia. La verificación de integridad de archivos es más efectiva cuando los archivos del sistema se comparan con una base de datos de referencia creada con un sistema conocido por su seguridad; esto ayuda a asegurar que la base de datos de referencia no se haya creado con archivos comprometidos. La base de datos de referencia debe almacenarse sin conexión para evitar que los atacantes comprometan el sistema y borren sus huellas modificando la base de datos.
Además, dado que los parches y otras actualizaciones modifican los archivos, la base de datos de sumas de comprobación debe mantenerse actualizada.

Para la verificación de la integridad de los archivos, se deben utilizar sumas de verificación criptográficas robustas, como el Algoritmo de Hash Seguro 1 (SHA-1), para garantizar la integridad de los datos almacenados en la base de datos de sumas de verificación. Las agencias federales están obligadas por la Norma Federal de Procesamiento de Información (FIPS) PUB 140-2, Requisitos de seguridad para módulos criptográficos11, a utilizar SHA (por ejemplo, SHA-1, SHA-256).

3.7 Resumen

La tabla 3-1 resume las principales capacidades de las técnicas de revisión analizadas en la sección 3.

Tabla 3-1. Técnicas de revisión

Técnica	Capacidades
Revisión de la documentación	• Evalúa las políticas y los procedimientos en cuanto a su precisión técnica e integridad.
Revisión de registros	• Proporciona información histórica sobre el uso, la configuración y las modificaciones del sistema. • Puede revelar posibles problemas y desviaciones de las políticas. • Revela deficiencias en los
Revisión del conjunto de reglas	controles de seguridad basados en reglas. • Evalúa la robustez de la
Configuración del sistema Revisar	configuración del sistema. • Valida que los sistemas estén configurados de acuerdo con la política de seguridad. • Supervisa el tráfico de red en el segmento local para capturar información
Análisis de red	como sistemas activos, sistemas operativos, protocolos de comunicación, servicios y aplicaciones. • Verifica el cifrado de las comunicaciones. • Identifica cambios
Comprobación de la integridad de los archivos	en archivos importantes; también puede identificar ciertos tipos de archivos no deseados, como herramientas de atacantes conocidas.

Cada técnica y sus combinaciones conllevan riesgos. Para garantizar su correcta y segura ejecución, cada evaluador debe poseer un nivel básico de competencias. La tabla 3-2 ofrece directrices sobre las competencias mínimas necesarias para cada técnica presentada en la sección 3.

Tabla 3-2. Conjunto de habilidades básicas para técnicas de revisión

Técnica	Conjunto de habilidades básicas
Revisión de documentación.	Conocimientos generales de seguridad desde una perspectiva política.
Revisión de registros	Conocimiento de formatos de registro y capacidad para interpretar y analizar datos de registro; capacidad para utilizar herramientas automatizadas de análisis y correlación de registros.
Revisión del conjunto de reglas	Conocimiento de formatos y estructuras de conjuntos de reglas; capacidad para correlacionar y analizar conjuntos de reglas de diversos dispositivos.
Configuración del sistema Revisar	Conocimientos sobre configuración segura de sistemas, incluyendo el fortalecimiento del sistema operativo y la configuración de políticas de seguridad para diversos sistemas operativos; capacidad para utilizar herramientas automatizadas de prueba de configuración de seguridad.

11 La publicación FIPS PUB 140-2 está disponible en http://csrc.nist.gov/publications/PubsFIPS.html.

Técnica	Conjunto de habilidades básicas
Análisis de red	Conocimientos generales de protocolo de control de transmisión/protocolo de Internet (TCP/IP) y redes; capacidad para interpretar y analizar el tráfico de red; capacidad para implementar y utilizar herramientas de análisis de tráfico de red.
Comprobación de la integridad de los archivos	Conocimientos generales de sistemas de archivos; capacidad para utilizar herramientas automatizadas de comprobación de la integridad de los archivos e interpretar los resultados.

4. Técnicas de identificación y análisis de objetivos

Esta sección aborda las técnicas técnicas de identificación y análisis de objetivos, que se centran en la identificación de dispositivos activos y sus puertos y servicios asociados, y en el análisis de los mismos en busca de posibles vulnerabilidades.
El evaluador utiliza esta información para seguir explorando dispositivos que validen la existencia de las vulnerabilidades.
Las organizaciones suelen utilizar técnicas no técnicas, ya sea como complemento o en lugar de las técnicas técnicas, para identificar los activos que se analizarán. Por ejemplo, pueden disponer de inventarios de activos u otras listas de activos que se pretenden analizar; otro ejemplo es cuando los evaluadores realizan una visita a las instalaciones para identificar activos que no se detectaron mediante técnicas técnicas, como equipos que estaban apagados o desconectados de la red cuando se utilizaron dichas técnicas.

Las técnicas de identificación y análisis de objetivos para el examen de seguridad de las aplicaciones se describen brevemente en el Apéndice C.

4.1 Descubrimiento de redes

El descubrimiento de red utiliza diversos métodos para detectar hosts activos y que responden en una red, identificar vulnerabilidades y comprender su funcionamiento. Existen técnicas tanto pasivas (de análisis) como activas (de prueba) para descubrir dispositivos en una red. Las técnicas pasivas utilizan un analizador de red para monitorizar el tráfico y registrar las direcciones IP de los hosts activos, pudiendo informar sobre los puertos en uso y los sistemas operativos detectados. El descubrimiento pasivo también permite identificar las relaciones entre hosts —incluyendo qué hosts se comunican entre sí, la frecuencia de dicha comunicación y el tipo de tráfico— y suele realizarse desde un host en la red interna, desde donde se puede monitorizar la comunicación entre hosts. Esto se lleva a cabo sin enviar ningún paquete de sondeo. El descubrimiento pasivo requiere más tiempo para recopilar información que el descubrimiento activo, y los hosts que no envían ni reciben tráfico durante el periodo de monitorización podrían no ser detectados.

Las técnicas activas envían varios tipos de paquetes de red, como pings del Protocolo de Mensajes de Control de Internet (ICMP), para solicitar respuestas de los hosts de la red, generalmente mediante el uso de una herramienta automatizada.
Una actividad, conocida como identificación del sistema operativo, permite al evaluador determinar el sistema operativo del sistema enviándole una combinación de tráfico de red normal, anómalo e ilegal. Otra actividad consiste en enviar paquetes a números de puerto comunes para generar respuestas que indiquen que los puertos están activos. La herramienta analiza las respuestas de estas actividades y las compara con características conocidas de paquetes de sistemas operativos y servicios de red específicos, lo que le permite identificar hosts, los sistemas operativos que ejecutan, sus puertos y el estado de estos. Esta información se puede utilizar para diversos fines, como recopilar información sobre objetivos para pruebas de penetración, generar mapas de topología, determinar configuraciones de firewall e IDS y descubrir vulnerabilidades en sistemas y configuraciones de red.

Las herramientas de descubrimiento de red ofrecen diversas formas de obtener información mediante escaneo. Los firewalls empresariales y los sistemas de detección de intrusiones pueden identificar numerosos escaneos, especialmente aquellos que utilizan los paquetes más sospechosos (p. ej., escaneo SYN/FIN, escaneo NULL). Los evaluadores que planeen realizar el descubrimiento a través de firewalls y sistemas de detección de intrusiones deben considerar qué tipos de escaneo tienen más probabilidades de proporcionar resultados sin llamar la atención de los administradores de seguridad, y cómo realizar escaneos de forma más sigilosa (por ejemplo, más lentamente o desde diversas direcciones IP de origen) para aumentar sus posibilidades de éxito. Asimismo, deben ser cautelosos al seleccionar los tipos de escaneo para sistemas antiguos, en particular aquellos con seguridad deficiente, ya que algunos escaneos pueden provocar fallos en el sistema.
Por lo general, cuanto más se acerque el escaneo a la actividad normal, menos probable es que cause problemas operativos.

El descubrimiento de red también puede detectar dispositivos no autorizados o fraudulentos que operan en una red. Por ejemplo, una organización que utiliza solo unos pocos sistemas operativos podría identificar rápidamente dispositivos fraudulentos que utilizan

Existen diferentes tipos. Una vez identificado un dispositivo no autorizado conectado por cable,[12] se puede localizar utilizando los mapas de red existentes y la información ya recopilada sobre su actividad de red para identificar el switch al que está conectado. Puede ser necesario generar actividad de red adicional con el dispositivo no autorizado —como pings— para encontrar el switch correcto. El siguiente paso es identificar el puerto del switch asociado al dispositivo no autorizado y rastrear físicamente el cable que conecta dicho puerto al dispositivo.

Existen diversas herramientas para el descubrimiento de redes, y cabe destacar que muchas de ellas también pueden utilizarse para el análisis pasivo de tráfico de red y el escaneo de puertos. La mayoría ofrece una interfaz gráfica de usuario (GUI), y algunas también una interfaz de línea de comandos. Aprender a usar las interfaces de línea de comandos puede llevar más tiempo que con las GUI, debido a la cantidad de comandos y parámetros que especifican las pruebas que debe realizar la herramienta y que un analista debe conocer para utilizarla eficazmente. Además, se han creado módulos para herramientas de código abierto que permiten a los analistas interpretar fácilmente los resultados. Por ejemplo, al combinar las capacidades de salida XML de una herramienta, un poco de programación y una base de datos, se crea una herramienta más potente capaz de monitorizar la red en busca de servicios y máquinas no autorizados. La mejor manera de aprender la función de los comandos y cómo combinarlos es con la ayuda de un ingeniero de seguridad con experiencia. La mayoría de los profesionales de TI con experiencia, incluidos los administradores de sistemas y otros ingenieros de redes, deberían poder interpretar los resultados, pero trabajar con las herramientas de descubrimiento en sí es más eficiente si lo realiza un ingeniero.

Algunas de las ventajas del descubrimiento activo, en comparación con el descubrimiento pasivo, son que la evaluación puede realizarse desde una red diferente y, por lo general, requiere poco tiempo para recopilar información. En el descubrimiento pasivo, garantizar que se capturen todos los hosts requiere que el tráfico pase por todos los puntos, lo que puede consumir mucho tiempo, especialmente en redes empresariales de gran tamaño.

Una desventaja del descubrimiento activo es que tiende a generar ruido en la red, lo que a veces provoca latencia. Dado que el descubrimiento activo envía consultas para recibir respuestas, esta actividad adicional en la red podría ralentizar el tráfico o provocar la pérdida de paquetes en redes mal configuradas si se realiza a gran escala. El descubrimiento activo también puede activar alertas del IDS, ya que, a diferencia del descubrimiento pasivo, revela su origen. La capacidad de descubrir correctamente todos los sistemas de la red puede verse afectada por entornos con segmentos de red protegidos y dispositivos y técnicas de seguridad perimetral. Por ejemplo, un entorno que utiliza traducción de direcciones de red (NAT), que permite a las organizaciones tener direcciones IP internas no enrutadas públicamente que se traducen a un conjunto diferente de direcciones IP públicas para el tráfico externo, puede no descubrirse con precisión desde puntos externos a la red o desde segmentos protegidos. Los firewalls personales y los firewalls de host en los dispositivos objetivo también pueden bloquear el tráfico de descubrimiento.

Es posible recibir información errónea al intentar provocar actividad en los dispositivos. La detección activa proporciona información a partir de la cual deben extraerse conclusiones sobre la configuración de la red objetivo.

Tanto en la detección pasiva como en la activa, la información recibida rara vez es completamente precisa. Por ejemplo, solo se identifican los hosts que están encendidos y conectados durante la detección activa; si los sistemas o un segmento de la red están fuera de línea durante la evaluación, existe la posibilidad de que se produzca una gran omisión en la detección de dispositivos. Si bien la detección pasiva solo encuentra dispositivos que transmiten o reciben comunicaciones durante el período de detección, productos como el software de administración de redes pueden proporcionar capacidades de detección continua y generar alertas automáticamente cuando se detecta un nuevo dispositivo en la red.

La detección continua puede escanear rangos de direcciones IP en busca de nuevas direcciones o supervisar nuevas solicitudes de direcciones IP. Además, muchas herramientas de descubrimiento pueden programarse para ejecutarse regularmente, por ejemplo, una vez cada cierto número de días a una hora determinada. Esto proporciona resultados más precisos que ejecutar estas herramientas esporádicamente.

[12] Consulte la Sección 4.4 para obtener información sobre cómo localizar dispositivos inalámbricos no autorizados.

4.2 Identificación de puertos y servicios de red

La identificación de puertos y servicios de red implica el uso de un escáner de puertos para identificar los puertos y servicios de red que operan en hosts activos, como FTP y HTTP, y la aplicación que ejecuta cada servicio identificado, como Microsoft Internet Information Server (IIS) o Apache para el servicio HTTP.
Las organizaciones deben realizar la identificación de puertos de red y servicios para identificar los hosts si esto no se ha hecho ya por otros medios (por ejemplo, el descubrimiento de red), y marcar los servicios potencialmente vulnerables.
Esta información puede utilizarse para determinar los objetivos de las pruebas de penetración.

Todos los escáneres básicos pueden identificar hosts activos y puertos abiertos, pero algunos también proporcionan información adicional sobre los hosts escaneados. La información recopilada durante un escaneo de puertos abiertos puede ayudar a identificar el sistema operativo objetivo mediante un proceso denominado huella digital del sistema operativo. Por ejemplo, si un host tiene abiertos los puertos TCP 135, 139 y 445, probablemente se trate de un host Windows o posiblemente de un host Unix con Samba. Otros elementos, como la generación del número de secuencia de paquetes TCP y las respuestas a los paquetes, también pueden proporcionar información.
También proporcionan una pista para identificar el sistema operativo. Sin embargo, la identificación del sistema operativo no es infalible. Por ejemplo, los cortafuegos bloquean ciertos puertos y tipos de tráfico, y los administradores de sistemas pueden configurar sus sistemas para que respondan de forma no estándar y así ocultar el verdadero sistema operativo.

Algunos escáneres pueden ayudar a identificar la aplicación que se ejecuta en un puerto específico mediante un proceso llamado identificación de servicios. Muchos escáneres utilizan un archivo de servicios que enumera los números de puerto comunes y los servicios asociados típicos; por ejemplo, un escáner que identifica que el puerto TCP 80 está abierto en un host puede informar que un servidor web está escuchando en ese puerto. Sin embargo, se requieren pasos adicionales para confirmar esta información.
Algunos escáneres pueden iniciar comunicaciones con un puerto observado y analizarlas para determinar qué servicio se está utilizando, a menudo comparando la actividad observada con un repositorio de información sobre servicios comunes e implementaciones de servicios. Estas técnicas también pueden utilizarse para identificar la aplicación y su versión, como por ejemplo, qué software de servidor web se está utilizando; este proceso se conoce como escaneo de versiones. Una forma común de escaneo de versiones, llamada captura de banners, consiste en capturar la información de los banners transmitidos por el puerto remoto cuando se inicia una conexión. Esta información puede incluir el tipo y la versión de la aplicación, e incluso el tipo y la versión del sistema operativo. El escaneo de versiones no es infalible, ya que un administrador preocupado por la seguridad puede alterar los banners transmitidos u otras características con la intención de ocultar la verdadera naturaleza del servicio. Sin embargo, el escaneo de versiones es mucho más preciso que simplemente basarse en el archivo de servicios de un escáner.

Los modelos de escáner admiten diversos métodos de escaneo, cada uno con sus ventajas y desventajas, las cuales suelen explicarse en su documentación. Por ejemplo, algunos escáneres funcionan mejor escaneando a través de firewalls, mientras que otros son más adecuados para escaneos dentro del firewall. Los resultados variarán según el escáner de puertos utilizado. Algunos escáneres responden simplemente indicando si un puerto está abierto o cerrado, mientras que otros ofrecen información adicional (por ejemplo, si está filtrado o no) que puede ayudar al analista a determinar qué otros tipos de escaneo serían útiles para obtener información adicional.

La identificación de puertos y servicios de red suele utilizar las direcciones IP obtenidas mediante el descubrimiento de red para identificar los dispositivos a escanear. Los escaneos de puertos también pueden ejecutarse de forma independiente en bloques completos de direcciones IP; en este caso, el escaneo de puertos realiza el descubrimiento de red por defecto identificando los hosts activos en la red. El resultado del descubrimiento de red y la identificación de puertos y servicios es una lista de todos los dispositivos activos que operan en el espacio de direcciones y que respondieron a la herramienta de escaneo de puertos, junto con los puertos que respondieron.
Podrían existir otros dispositivos activos que no respondieron al escaneo, como aquellos protegidos por cortafuegos o apagados. Los evaluadores pueden intentar encontrar estos dispositivos escaneándolos ellos mismos.

Colocar el escáner en un segmento que pueda acceder a los dispositivos, o intentar evadir el cortafuegos mediante el uso de tipos de escaneo alternativos (por ejemplo, escaneo SYN/FIN o Xmas).13

Se recomienda que, si se van a utilizar tanto el escaneo externo como el interno y los evaluadores realizan las pruebas a ciegas, el escaneo externo se realice primero. De esta forma, los registros se pueden revisar y comparar antes y durante las pruebas internas. Al realizar el escaneo externo, los evaluadores pueden utilizar técnicas de sigilo para que los paquetes atraviesen los cortafuegos sin ser detectados por los sistemas IDS e IPS.¹⁴ Se recomienda el uso de herramientas que emplean técnicas de fragmentación, duplicación, superposición, desorden y temporización para alterar los paquetes y que se integren mejor en el tráfico normal.

Las pruebas internas suelen emplear métodos de escaneo menos agresivos, ya que se bloquean con menor frecuencia que los escaneos externos. El uso de escaneos más agresivos internamente aumenta significativamente las probabilidades de interrumpir las operaciones sin que ello necesariamente mejore los resultados. La capacidad de escanear una red con paquetes personalizados también resulta útil para las pruebas internas, puesto que la detección de vulnerabilidades específicas requiere paquetes altamente personalizados. Las herramientas con capacidad de generar paquetes son de gran ayuda en este proceso. Una vez generados, los paquetes se pueden enviar a través de un segundo programa de escaneo que recopilará los resultados. Dado que los paquetes personalizados pueden desencadenar un ataque de denegación de servicio (DoS), este tipo de prueba debe realizarse durante periodos de baja actividad en la red, como por la noche o los fines de semana.

Si bien los escáneres de puertos identifican hosts activos, sistemas operativos, puertos, servicios y aplicaciones, no detectan vulnerabilidades. Se requiere una investigación adicional para confirmar la presencia de protocolos inseguros (p. ej., TFTP, telnet), malware, aplicaciones no autorizadas y servicios vulnerables. Para identificar servicios vulnerables, el evaluador compara los números de versión identificados con una lista de versiones vulnerables conocidas o realiza un escaneo automatizado de vulnerabilidades, como se describe en la sección 4.3. Con los escáneres de puertos, el proceso de escaneo está altamente automatizado, pero la interpretación de los datos escaneados no lo está.

Si bien el escaneo de puertos puede interrumpir las operaciones de red al consumir ancho de banda y ralentizar los tiempos de respuesta, permite a una organización garantizar que sus hosts estén configurados para ejecutar únicamente servicios de red autorizados. El software de escaneo debe seleccionarse cuidadosamente para minimizar las interrupciones operativas.
El escaneo de puertos también puede realizarse fuera del horario laboral para minimizar el impacto en las operaciones.

4.3 Escaneo de vulnerabilidades

Al igual que la identificación de puertos y servicios de red, el escaneo de vulnerabilidades identifica hosts y sus atributos (por ejemplo, sistemas operativos, aplicaciones, puertos abiertos), pero también intenta identificar vulnerabilidades en lugar de depender de la interpretación humana de los resultados del escaneo. Muchos escáneres de vulnerabilidades están equipados para aceptar resultados de detección de red e identificación de puertos y servicios, lo que reduce el trabajo necesario para el escaneo de vulnerabilidades. Además, algunos escáneres pueden realizar su propia detección de red e identificación de puertos y servicios. El escaneo de vulnerabilidades puede ayudar a identificar versiones de software obsoletas, parches faltantes y configuraciones erróneas, y a validar el cumplimiento o las desviaciones de la política de seguridad de una organización. Esto se logra identificando los sistemas operativos y las principales aplicaciones de software que se ejecutan en los hosts y comparándolos con la información sobre vulnerabilidades conocidas almacenada en las bases de datos de vulnerabilidades de los escáneres.

Los escáneres de vulnerabilidades pueden:

- Verificar el cumplimiento de las políticas de seguridad y uso de la aplicación del host.

[13] Muchos cortafuegos pueden reconocer y bloquear varios tipos de escaneo alternativos, por lo que es posible que los evaluadores no puedan utilizarlos para evadir los cortafuegos en muchos entornos.

[14] Esto puede resultar especialmente útil para mejorar el ajuste y la configuración de los IDS y los IPS.

Proporcionar información sobre los objetivos para las pruebas de penetración

Proporcionar información sobre cómo mitigar las vulnerabilidades descubiertas.

Los escáneres de vulnerabilidades pueden ejecutarse en un equipo tanto localmente como desde la red. Algunos escáneres de red cuentan con credenciales de administrador en equipos individuales y pueden extraer información sobre vulnerabilidades utilizando dichas credenciales. Otros escáneres de red no disponen de estas credenciales y deben realizar escaneos de red para localizar equipos y, posteriormente, analizarlos en busca de vulnerabilidades. En estos casos, el escaneo de red se utiliza principalmente para descubrir la red e identificar puertos abiertos y vulnerabilidades relacionadas; en la mayoría de los casos, no está limitado por el sistema operativo de los equipos objetivo.
El escaneo de red sin credenciales de host puede realizarse tanto interna como externamente; si bien el escaneo interno suele descubrir más vulnerabilidades que el externo, es importante realizar pruebas desde ambas perspectivas. El escaneo externo debe lidiar con los dispositivos de seguridad perimetral que bloquean el tráfico, lo que limita a los evaluadores a escanear únicamente los puertos autorizados para el paso de datos.

Los evaluadores que realizan escaneos externos pueden encontrar desafíos similares a los de la detección de redes, como el uso de NAT o firewalls personales y de host. Para superar los desafíos de NAT y realizar escaneos de red exitosos, pueden solicitar al administrador del firewall que habilite el reenvío de puertos en direcciones IP específicas o grupos de direcciones, si el firewall lo admite, o solicitar acceso a la red detrás del dispositivo que realiza NAT. También pueden solicitar que se configuren los firewalls personales o de host para permitir el tráfico desde las direcciones IP del sistema de prueba durante el período de evaluación. Estas medidas proporcionarán a los evaluadores una mayor comprensión de la red, pero no reflejan con precisión las capacidades de un atacante externo, aunque pueden ofrecer una mejor indicación de las capacidades disponibles para un empleado malintencionado o un atacante externo con acceso a otro host en la red interna.

Los evaluadores también pueden realizar escaneos en hosts individuales.

Para el escaneo de vulnerabilidades locales, se instala un escáner en cada host que se va a analizar. Esto se realiza principalmente para identificar errores de configuración y vulnerabilidades en el sistema operativo y las aplicaciones del host, tanto explotables a través de la red como localmente. El escaneo local permite detectar vulnerabilidades con mayor detalle que el escaneo basado en la red, ya que generalmente requiere acceso local al host y una cuenta de administrador o de superusuario. Algunos escáneres también ofrecen la capacidad de corregir errores de configuración locales.

Un escáner de vulnerabilidades es una forma relativamente rápida y sencilla de cuantificar la exposición de una organización a vulnerabilidades superficiales. Una vulnerabilidad superficial es una debilidad que existe de forma aislada, independiente de otras vulnerabilidades. El comportamiento y los resultados del sistema en respuesta a los patrones de ataque enviados por el escáner se comparan con las firmas características de vulnerabilidades conocidas, y la herramienta informa de cualquier coincidencia encontrada. Además del escaneo basado en firmas, algunos escáneres de vulnerabilidades intentan simular los patrones de ataque de reconocimiento utilizados para detectar vulnerabilidades expuestas y explotables, e informan de las vulnerabilidades encontradas cuando estas técnicas tienen éxito.

Una dificultad para identificar el nivel de riesgo de las vulnerabilidades radica en que rara vez se presentan de forma aislada. Por ejemplo, podría haber varias vulnerabilidades de bajo riesgo que, combinadas, presenten un riesgo mayor.
Los escáneres no pueden detectar vulnerabilidades que se revelan únicamente como resultado de combinaciones potencialmente infinitas de patrones de ataque. La herramienta puede asignar un riesgo bajo a cada vulnerabilidad, lo que genera una falsa sensación de seguridad en las medidas implementadas. Un método más fiable para identificar el riesgo de las vulnerabilidades en su conjunto es mediante pruebas de penetración, que se abordan en la sección 5.2.

Otro problema al identificar el nivel de riesgo de las vulnerabilidades es que los escáneres de vulnerabilidades suelen utilizar métodos propios para definir dichos niveles. Por ejemplo, un escáner podría usar los niveles bajo, medio y alto, mientras que otro podría usar los niveles informativo, bajo, medio, alto y crítico. Esto dificulta la comparación de los resultados entre distintos escáneres. Además, los niveles de riesgo asignados por un escáner pueden no reflejar el riesgo real para la organización; por ejemplo, un escáner podría...

Se clasifica un servidor FTP como de riesgo moderado porque transmite contraseñas en texto plano, pero si la organización solo lo utiliza como servidor público anónimo sin contraseñas, el riesgo real podría ser considerablemente menor. Los evaluadores deben determinar el nivel de riesgo adecuado para cada vulnerabilidad y no simplemente aceptar los niveles asignados por los escáneres de vulnerabilidades.

El escaneo de vulnerabilidades basado en la red presenta importantes limitaciones. Al igual que el rastreo y la detección de tráfico de red, este tipo de escaneo solo descubre vulnerabilidades en sistemas activos. Generalmente, esto cubre vulnerabilidades superficiales y no permite evaluar el nivel de riesgo general de una red escaneada. Si bien el proceso está altamente automatizado, los escáneres de vulnerabilidades pueden tener una alta tasa de falsos positivos (es decir, reportan vulnerabilidades inexistentes). Un experto en seguridad de redes y sistemas operativos debe interpretar los resultados. Además, dado que el escaneo de vulnerabilidades basado en la red requiere más información que el escaneo de puertos para identificar de forma fiable las vulnerabilidades en un host, tiende a generar mucho más tráfico de red. Esto puede tener un impacto negativo en los hosts o la red escaneada, o en los segmentos de red por donde transita el tráfico de escaneo. Muchos escáneres de vulnerabilidades también incluyen pruebas de red para ataques DoS que, en manos de un evaluador inexperto, pueden tener un impacto negativo significativo en los hosts escaneados. Los escáneres a menudo permiten suprimir todas las pruebas de ataques DoS para reducir el riesgo de afectar a los hosts durante las pruebas.

Otra limitación importante de los escáneres de vulnerabilidades es que, al igual que los antivirus y los sistemas de detección de intrusiones (IDS), dependen de un repositorio de firmas. Esto exige que los evaluadores actualicen estas firmas con frecuencia para que el escáner pueda reconocer las vulnerabilidades más recientes. Antes de ejecutar cualquier escáner, el evaluador debe instalar las últimas actualizaciones de su base de datos de vulnerabilidades. Algunas bases de datos de escáneres de vulnerabilidades se actualizan con mayor regularidad que otras; esta frecuencia de actualización debe ser un factor clave a la hora de seleccionar un escáner de vulnerabilidades.

La mayoría de los escáneres de vulnerabilidades permiten al evaluador realizar distintos niveles de escaneo, con diferentes grados de exhaustividad. Si bien un escaneo más completo puede detectar un mayor número de vulnerabilidades, puede ralentizar el proceso general. Un escaneo menos exhaustivo puede ser más rápido, pero solo identifica vulnerabilidades conocidas. En general, se recomienda que los evaluadores realicen un escaneo de vulnerabilidades exhaustivo si los recursos lo permiten.

El escaneo de vulnerabilidades es una actividad laboriosa que requiere una alta intervención humana para interpretar los resultados. Además, puede interrumpir las operaciones de la red al consumir ancho de banda y ralentizar los tiempos de respuesta. Sin embargo, es fundamental para garantizar que las vulnerabilidades se mitiguen antes de que sean descubiertas y explotadas por atacantes.

Al igual que todas las herramientas basadas en patrones y firmas, los escáneres de vulnerabilidades de aplicaciones suelen tener altas tasas de falsos positivos. Los evaluadores deben configurar y calibrar sus escáneres para minimizar tanto los falsos positivos como los falsos negativos, e interpretar los resultados de forma significativa para identificar las vulnerabilidades reales. Los escáneres también presentan las altas tasas de falsos negativos que caracterizan a otras herramientas basadas en firmas; sin embargo, las vulnerabilidades que pasan desapercibidas para los escáneres automatizados pueden detectarse utilizando varios escáneres de vulnerabilidades o pruebas adicionales. Una práctica común es utilizar varios escáneres, lo que permite a los evaluadores comparar los resultados.

4.4 Escaneo inalámbrico

Las tecnologías inalámbricas, en su forma más simple, permiten que uno o más dispositivos se comuniquen sin necesidad de conexiones físicas como cables de red o periféricos. Abarcan desde tecnologías sencillas como teclados y ratones inalámbricos hasta complejas redes de telefonía móvil y redes de área local inalámbricas (WLAN) empresariales. A medida que aumenta el número y la disponibilidad de dispositivos inalámbricos,

Es importante que las organizaciones prueben y protejan activamente sus entornos inalámbricos empresariales.15 Los escaneos inalámbricos pueden ayudar a las organizaciones a determinar acciones correctivas para mitigar los riesgos que plantean las tecnologías habilitadas para la tecnología inalámbrica.

Al planificar evaluaciones técnicas de seguridad inalámbrica, se deben tener en cuenta los siguientes factores del entorno de la organización:

La ubicación de la instalación que se está escaneando, ya que la proximidad física de un edificio a una zona pública (por ejemplo, calles y zonas comunes públicas) o su ubicación en una zona metropolitana concurrida puede aumentar el riesgo de amenazas inalámbricas.

El nivel de seguridad de los datos que se transmitirán utilizando tecnologías inalámbricas

La frecuencia con la que los dispositivos inalámbricos se conectan y desconectan del entorno, y los niveles de tráfico típicos de dichos dispositivos (por ejemplo, actividad ocasional o bastante constante): esto se debe a que solo los dispositivos inalámbricos activos son detectables durante un escaneo inalámbrico.

Las implementaciones existentes de sistemas inalámbricos de detección y prevención de intrusiones (WIDPS16) pueden recopilar ya la mayor parte de la información que se obtendría mediante pruebas.

El escaneo inalámbrico debe realizarse mediante un dispositivo móvil con software de análisis inalámbrico instalado y configurado, como una computadora portátil, un dispositivo de mano o un dispositivo especializado. El software o la herramienta de escaneo debe permitir al operador configurar el dispositivo para escaneos específicos y escanear tanto en modo pasivo como activo. Asimismo, el operador debe poder configurar el software de escaneo para identificar desviaciones de los requisitos de configuración de seguridad inalámbrica de la organización.

La herramienta de escaneo inalámbrico debe ser capaz de escanear todos los canales IEEE 802.11a/b/g/n, tanto nacionales como internacionales. En algunos casos, el dispositivo también debería estar equipado con una antena externa para proporcionar una mayor capacidad de captura de radiofrecuencia (RF). La compatibilidad con otras tecnologías inalámbricas, como Bluetooth, ayudará a evaluar la presencia de amenazas y vulnerabilidades inalámbricas adicionales. Cabe destacar que los dispositivos que utilicen tecnología no estándar o frecuencias fuera del rango de RF de la herramienta de escaneo no serán detectados ni reconocidos correctamente. Una herramienta como un analizador de espectro de RF ayudará a las organizaciones a identificar las transmisiones que se produzcan dentro del rango de frecuencia del analizador. Los analizadores de espectro generalmente analizan un amplio rango de frecuencia (por ejemplo, de 3 a 18 GHz); si bien estos dispositivos no analizan el tráfico, permiten al evaluador determinar la actividad inalámbrica dentro de un rango de frecuencia específico y adaptar las pruebas y análisis adicionales en consecuencia.

Algunos dispositivos también permiten la creación de mapas y la localización física mediante una herramienta de mapeo, y en algunos casos, admiten mapas basados en el Sistema de Posicionamiento Global (GPS). Las sofisticadas herramientas de escaneo inalámbrico permiten importar un plano o mapa para facilitar la localización física de los dispositivos detectados. (Cabe destacar que el GPS tiene capacidades limitadas en interiores).

Las personas con sólidos conocimientos de redes inalámbricas, especialmente de las tecnologías IEEE 802.11a/b/g/n, deben operar las herramientas de escaneo inalámbrico. Estos operadores deben recibir capacitación sobre la funcionalidad y las capacidades de las herramientas y el software de escaneo para comprender mejor la información capturada y ser más capaces de identificar posibles amenazas o actividades maliciosas.

---

15 Para conocer las medidas adecuadas para proteger las WLAN basadas en IEEE 802.11, consulte NIST SP 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, y NIST SP 800-48 Revisión 1, Guide to Securing Legacy IEEE 802.11 Wireless Networks, disponibles en http://csrc.nist.gov/publications/PubsSPs.html.

16 Para obtener más información, consulte NIST SP 800-94, Guía de sistemas de detección y prevención de intrusiones (IDPS), que está disponible en http://csrc.nist.gov/publications/PubsSPs.html.

Se deben emplear habilidades para analizar los datos y resultados obtenidos de los escaneos inalámbricos. Los operadores de herramientas de escaneo deben conocer otras señales de radiofrecuencia autorizadas para su uso dentro del área que se está escaneando.

4.4.1 Escaneo inalámbrico pasivo

Se recomienda realizar escaneos pasivos periódicamente para complementar las medidas de seguridad inalámbricas ya implementadas, como los sistemas de detección y prevención de intrusiones inalámbricas (WIDPS).[1] Las herramientas de escaneo inalámbrico que realizan escaneos completamente pasivos no transmiten datos ni afectan de ninguna manera el funcionamiento de los dispositivos inalámbricos desplegados. Al no transmitir datos, una herramienta de escaneo pasivo permanece indetectable para usuarios malintencionados y otros dispositivos. Esto reduce la probabilidad de que los usuarios eviten ser detectados desconectando o desactivando dispositivos inalámbricos no autorizados.

Las herramientas de escaneo pasivo capturan el tráfico inalámbrico que se transmite dentro del alcance de la antena de la herramienta. La mayoría de las herramientas proporcionan varios atributos clave sobre los dispositivos inalámbricos detectados, como el identificador del conjunto de servicios (SSID), el tipo de dispositivo, el canal, la dirección MAC, la intensidad de la señal y el número de paquetes transmitidos. Esta información permite evaluar la seguridad del entorno inalámbrico e identificar posibles dispositivos no autorizados y redes ad hoc no autorizadas dentro del alcance del dispositivo de escaneo. La herramienta de escaneo inalámbrico también debe poder analizar los paquetes capturados para determinar si existen anomalías operativas o amenazas.

Las herramientas de escaneo inalámbrico analizan cada canal/frecuencia IEEE 802.11a/b/g/n por separado, a menudo durante solo unos cientos de milisegundos. Es posible que la herramienta de escaneo pasivo no reciba todas las transmisiones en un canal específico. Por ejemplo, podría estar analizando el canal 1 justo en el momento en que un dispositivo inalámbrico transmitió un paquete en el canal 5. Por ello, es importante configurar el tiempo de permanencia de la herramienta lo suficientemente largo para capturar paquetes, pero lo suficientemente corto para analizar eficientemente cada canal. La configuración del tiempo de permanencia dependerá del dispositivo o herramienta utilizada para realizar los escaneos inalámbricos. Además, el personal de seguridad que realiza los escaneos debe moverse lentamente por el área analizada para reducir la cantidad de dispositivos que no se detectan.

Los dispositivos no autorizados pueden identificarse de varias maneras mediante escaneo pasivo:

- La dirección MAC de un dispositivo inalámbrico detectado indica el fabricante de su interfaz inalámbrica. Si una organización solo utiliza interfaces inalámbricas de los fabricantes A y B, la presencia de interfaces de cualquier otro fabricante indica la posible existencia de dispositivos no autorizados.
- Si una organización cuenta con registros precisos de sus dispositivos inalámbricos desplegados, los evaluadores pueden comparar las direcciones MAC de los dispositivos detectados con las de los dispositivos autorizados. La mayoría de las herramientas de escaneo permiten a los evaluadores ingresar una lista de dispositivos autorizados. Dado que las direcciones MAC pueden ser falsificadas, los evaluadores no deben asumir que las direcciones MAC de los dispositivos detectados son correctas; sin embargo, verificar las direcciones MAC puede identificar dispositivos no autorizados que no utilizan suplantación de identidad.
- Los dispositivos no autorizados pueden utilizar SSID que no están autorizados por la organización.
- Algunos dispositivos no autorizados pueden usar SSID autorizados por la organización pero que no cumplen con sus requisitos de configuración de seguridad inalámbrica.

Se debe revisar la intensidad de la señal de los posibles dispositivos no autorizados para determinar si se encuentran dentro de las instalaciones o en el área que se está escaneando. Los dispositivos que operan fuera de las instalaciones o en el área que se está escaneando deben ser detectados como dispositivos no autorizados.

[17] En ciertos entornos, la implementación de WIDPS podría realizar la mayoría de las mismas funciones que el escaneo inalámbrico pasivo. Algunos productos WIDPS ofrecen sensores móviles similares a la configuración del dispositivo de escaneo inalámbrico descrita en la Sección 4.4. Las organizaciones con implementaciones de WIDPS deben usar las técnicas de escaneo inalámbrico descritas en esta publicación para complementar, no duplicar, la funcionalidad de WIDPS.

Los límites de la organización aún podrían plantear riesgos significativos, ya que los dispositivos de la organización podrían conectarse inadvertidamente a ellos.

4.4.2 Escaneo inalámbrico activo

Las organizaciones pueden ir más allá del escaneo pasivo de redes inalámbricas y realizar escaneos activos. Estos se basan en la información recopilada durante los escaneos pasivos e intentan conectarse a los dispositivos detectados para realizar pruebas de penetración o de vulnerabilidad. Por ejemplo, las organizaciones pueden realizar escaneos activos de sus dispositivos inalámbricos autorizados para garantizar que cumplan con los requisitos de configuración de seguridad inalámbrica, incluidos los mecanismos de autenticación, el cifrado de datos y el acceso administrativo, si esta información no está disponible por otros medios.

Las organizaciones deben ser cautelosas al realizar escaneos activos para asegurarse de no escanear inadvertidamente dispositivos pertenecientes a organizaciones vecinas o gestionados por ellas que se encuentren dentro del alcance. Es importante evaluar la ubicación física de los dispositivos antes de escanearlos. Asimismo, las organizaciones deben tener precaución al realizar escaneos activos de dispositivos no autorizados que parezcan estar operando dentro de sus instalaciones.
Estos dispositivos podrían pertenecer a un visitante de la organización que, inadvertidamente, tiene habilitado el acceso inalámbrico, o a una organización vecina con un dispositivo que se encuentra cerca, pero no dentro, de las instalaciones de la organización.
En general, las organizaciones deberían centrarse en identificar y localizar posibles dispositivos maliciosos en lugar de realizar escaneos activos de dichos dispositivos.

Las organizaciones pueden utilizar escaneo activo al realizar pruebas de penetración en sus propios dispositivos inalámbricos. Existen herramientas que emplean ataques y funciones predefinidas, intentan eludir las medidas de seguridad implementadas y evalúan el nivel de seguridad de los dispositivos. Por ejemplo, las herramientas utilizadas para realizar pruebas de penetración inalámbricas intentan conectarse a los puntos de acceso (AP) mediante diversos métodos para eludir las configuraciones de seguridad. Si la herramienta logra acceder al AP, puede obtener información e identificar las redes cableadas y los dispositivos inalámbricos a los que está conectado. Algunas herramientas activas también pueden identificar vulnerabilidades en los dispositivos cliente inalámbricos o realizar pruebas de vulnerabilidad en redes cableadas, como se describe en la Sección 4.

Mientras se realiza un escaneo activo, se pueden monitorizar los sistemas WIDPS de la organización para evaluar sus capacidades y rendimiento. Según los objetivos de la evaluación, los evaluadores que realizan estos escaneos podrían necesitar informar a los administradores de los sistemas WIDPS y de la red inalámbrica sobre los escaneos pendientes para prepararlos ante posibles alarmas y alertas. Además, algunos sistemas WIDPS se pueden configurar para ignorar las alarmas y alertas generadas por un dispositivo específico, como uno utilizado para realizar el escaneo.

Las herramientas y los procesos para identificar dispositivos no autorizados y vulnerabilidades en redes cableadas también pueden utilizarse para identificar dispositivos inalámbricos no autorizados o mal configurados. El escaneo de la red cableada es otro proceso que puede realizarse para descubrir, y posiblemente localizar, dispositivos inalámbricos no autorizados. Las secciones 3.5 y 4.1 tratan sobre el escaneo de la red cableada.

4.4.3 Seguimiento de la ubicación de dispositivos inalámbricos

El personal de seguridad que opera la herramienta de escaneo inalámbrica debe intentar localizar dispositivos sospechosos.
Las señales de radiofrecuencia se propagan en función del entorno, por lo que es importante que el operador comprenda cómo la tecnología inalámbrica sustenta este proceso. Las funciones de mapeo son útiles en este sentido, pero los factores principales necesarios para que esta capacidad sea viable son un operador con conocimientos y una antena inalámbrica adecuada.

Si durante el escaneo inalámbrico se descubren y localizan físicamente dispositivos no autorizados, el personal de seguridad debe asegurarse de que se sigan las políticas y los procesos específicos sobre cómo manejar el dispositivo no autorizado, tales como:

Se puede optar por apagar el dispositivo, reconfigurarlo para que cumpla con las políticas de la organización o retirarlo por completo. Si se decide retirarlo, el personal de seguridad debe evaluar la actividad del dispositivo no autorizado antes de su confiscación. Esto se puede hacer mediante la monitorización de las transmisiones y los intentos de acceso al dispositivo.

Si no se pueden localizar los dispositivos inalámbricos detectados durante el escaneo, el personal de seguridad debe intentar usar un WIDPS para ayudar a localizarlos. Esto requiere que el WIDPS localice una dirección MAC específica detectada durante el escaneo. Los WIDPS implementados correctamente deberían poder ayudar al personal de seguridad a localizar estos dispositivos y, por lo general, implican el uso de varios sensores WIDPS para aumentar la precisión en la identificación de la ubicación. Dado que el WIDPS solo podrá localizar un dispositivo dentro de un radio de varios metros, es posible que aún se necesite una herramienta de escaneo inalámbrico para determinar con exactitud su ubicación.

4.4.4 Escaneo Bluetooth

Para las organizaciones que desean confirmar el cumplimiento de sus requisitos de seguridad Bluetooth, se recomienda realizar un escaneo pasivo de dispositivos inalámbricos con Bluetooth para evaluar su posible presencia y actividad. Debido al corto alcance de Bluetooth (un promedio de 9 metros, aunque algunos dispositivos tienen un alcance de tan solo 1 metro), el escaneo de dispositivos puede resultar difícil y lento.
Los evaluadores deben tener en cuenta las limitaciones de alcance al definir este tipo de escaneo.
Es posible que las organizaciones opten por realizar escaneos únicamente en las áreas de sus instalaciones accesibles al público, para comprobar si los atacantes podrían acceder a los dispositivos mediante Bluetooth, o bien, realizar escaneos en una muestra de ubicaciones físicas en lugar de en toda la instalación. Dado que muchos dispositivos con Bluetooth (como teléfonos móviles y asistentes digitales personales [PDA]) son móviles, podría ser necesario realizar escaneos pasivos varias veces durante un período de tiempo. Las organizaciones también deberían escanear cualquier infraestructura Bluetooth que implementen, como los puntos de acceso. Si se detectan puntos de acceso no autorizados, la organización deberá gestionarlos de acuerdo con las políticas y los procedimientos establecidos.

Existen diversas herramientas para probar activamente la seguridad y el funcionamiento de los dispositivos Bluetooth. Estas herramientas intentan conectarse a los dispositivos detectados y realizar ataques para obtener acceso y conectividad a dispositivos con Bluetooth de forma subrepticia. Los evaluadores deben ser extremadamente cautelosos al realizar escaneos activos debido a la probabilidad de escanear inadvertidamente dispositivos Bluetooth personales, que se encuentran en muchos entornos. Como regla general, los evaluadores solo deben usar el escaneo activo cuando tengan la certeza de que los dispositivos escaneados pertenecen a la organización. El escaneo activo se puede usar para evaluar el modo de seguridad en el que opera un dispositivo Bluetooth y la robustez de los números de identificación de contraseña (PIN) de Bluetooth. También se puede usar para verificar que estos dispositivos estén configurados con el nivel de potencia mínimo para reducir su alcance. Al igual que con los dispositivos no autorizados IEEE 802.11a/b/g, los dispositivos Bluetooth no autorizados deben gestionarse de acuerdo con las políticas y directrices establecidas.

4.5 Resumen

La Tabla 4-1 resume las principales capacidades de las técnicas de identificación y análisis de objetivos discutidas en la Sección 4.

Tabla 4-1. Técnicas de identificación y análisis de objetivos

Técnica	Capacidades
Descubrimiento de redes	• Detecta dispositivos activos • Identifica las rutas de comunicación y facilita la determinación de la red Arquitecturas •
Puerto de red y Identificación del servicio	Detecta dispositivos activos • Detecta puertos abiertos y servicios/aplicaciones asociados

Técnica	Capacidades
Escaneo de vulnerabilidades	• Identifica hosts y puertos abiertos • Identifica vulnerabilidades conocidas (nota: tiene una alta tasa de falsos positivos) • A menudo proporciona consejos sobre cómo mitigar las vulnerabilidades detectadas • Identifica
Escaneo inalámbrico	dispositivos inalámbricos no autorizados dentro del alcance de los escáneres • Detecta señales inalámbricas fuera del perímetro de una organización • Detecta posibles puertas traseras y otras violaciones de seguridad

Cada técnica y combinación de técnicas conlleva riesgos. Para garantizar su correcta y segura ejecución, cada evaluador debe poseer un nivel básico de competencias. La tabla 4-2 ofrece directrices sobre las competencias mínimas necesarias para cada técnica presentada en la sección 4.

Tabla 4-2. Conjunto de habilidades básicas para técnicas de identificación y análisis de objetivos

Técnica	Conjunto de habilidades básicas
Descubrimiento de redes	Conocimientos generales de TCP/IP y redes; capacidad para utilizar herramientas de detección de redes tanto pasivas como activas.
Puerto de red y Identificación del servicio	Conocimientos generales de TCP/IP y redes; conocimiento de puertos y protocolos para diversos sistemas operativos; capacidad para utilizar herramientas de escaneo de puertos; capacidad para interpretar los resultados de dichas herramientas.
Escaneo de vulnerabilidades	Conocimientos generales de TCP/IP y redes; conocimiento de puertos, protocolos, servicios y vulnerabilidades en diversos sistemas operativos; capacidad para utilizar herramientas automatizadas de escaneo de vulnerabilidades e interpretar/analizar los resultados.
Escaneo inalámbrico	Conocimientos generales de informática y transmisiones de radio, además de conocimientos específicos de protocolos, servicios y arquitecturas inalámbricas; capacidad para utilizar herramientas automatizadas de escaneo y análisis de tráfico inalámbrico.

5. Técnicas de validación de vulnerabilidades del objetivo

Esta sección aborda las técnicas de validación de vulnerabilidades en sistemas objetivo, las cuales utilizan la información obtenida de la identificación y el análisis del objetivo para explorar la existencia de vulnerabilidades potenciales. El objetivo es demostrar la existencia de una vulnerabilidad y evidenciar los riesgos de seguridad que se generan al explotarla. La validación de vulnerabilidades en sistemas objetivo implica el mayor riesgo en las evaluaciones, ya que estas técnicas tienen un mayor potencial de impacto en el sistema o la red objetivo que otras técnicas.

Las técnicas de validación de vulnerabilidades objetivo para las pruebas de seguridad de aplicaciones se analizan brevemente en el Apéndice C.

5.1 Descifrado de contraseñas

Cuando un usuario introduce una contraseña, se genera un hash de la misma y se compara con un hash almacenado de la contraseña real del usuario. Si los hashes coinciden, el usuario se autentica. El descifrado de contraseñas es el proceso de recuperar contraseñas a partir de hashes almacenados en un sistema informático o transmitidos por redes. Generalmente se realiza durante evaluaciones para identificar cuentas con contraseñas débiles.
El descifrado de contraseñas se realiza sobre hashes que se interceptan mediante un analizador de red durante su transmisión o se recuperan del sistema objetivo, lo que generalmente requiere acceso administrativo o físico al mismo. Una vez obtenidos estos hashes, un programa automatizado de descifrado genera rápidamente hashes adicionales hasta encontrar una coincidencia o hasta que el evaluador detiene el intento.

Un método para generar hashes es el ataque de diccionario, que utiliza todas las palabras de un diccionario o archivo de texto. En Internet existen numerosos diccionarios que abarcan idiomas principales y minoritarios, nombres, programas de televisión populares, etc. Otro método de descifrado es el ataque híbrido, que se basa en el método del diccionario añadiendo caracteres numéricos y simbólicos a las palabras. Dependiendo del programa de descifrado de contraseñas utilizado, este tipo de ataque puede probar diversas variantes, como sustituir letras por caracteres y números comunes (por ejemplo, p@ssword y h4ckme). Algunos también intentan añadir caracteres y números al principio y al final de las palabras (por ejemplo, password99, password$%).

Otro método para descifrar contraseñas es el de fuerza bruta . Este genera todas las contraseñas posibles hasta una longitud determinada y sus hashes asociados. Debido a la gran cantidad de posibilidades, descifrar una contraseña puede llevar meses. Si bien la fuerza bruta puede ser un proceso largo, suele ser mucho más rápido que el tiempo que especifican la mayoría de las políticas de contraseñas para su cambio. Por lo tanto, las contraseñas encontradas durante los ataques de fuerza bruta siguen siendo demasiado débiles. En teoría, todas las contraseñas pueden descifrarse mediante un ataque de fuerza bruta, con suficiente tiempo y capacidad de procesamiento, aunque esto podría llevar muchos años y requerir una gran potencia informática. Los analistas y atacantes suelen disponer de varias máquinas para distribuir la tarea de descifrar contraseñas, lo que reduce considerablemente el tiempo necesario.

El descifrado de contraseñas también puede realizarse con tablas arcoíris, que son tablas de búsqueda con hashes de contraseñas precalculados. Por ejemplo, se puede crear una tabla arcoíris que contenga todas las contraseñas posibles para una combinación de caracteres dada, hasta una longitud determinada. Los analistas pueden entonces buscar en la tabla los hashes de contraseñas que intentan descifrar. Las tablas arcoíris requieren una gran cantidad de espacio de almacenamiento y pueden tardar mucho tiempo en generarse, pero su principal inconveniente es que pueden ser ineficaces contra el hash de contraseñas que utiliza salting. El salting consiste en la inclusión de una información aleatoria en el proceso de hash de contraseñas para disminuir la probabilidad de que contraseñas idénticas generen el mismo hash. Las tablas arcoíris no producirán resultados correctos sin tener en cuenta el salting, pero esto aumenta drásticamente la cantidad de espacio de almacenamiento que requieren. Muchos sistemas operativos utilizan

Mecanismos de cifrado de contraseñas con sal para reducir la eficacia de las tablas arcoíris y otras formas de descifrado de contraseñas.

Durante una evaluación, se pueden ejecutar programas para descifrar contraseñas y así garantizar el cumplimiento de las políticas, verificando la composición aceptable de las contraseñas. Por ejemplo, si la organización tiene una política de caducidad de contraseñas, se pueden ejecutar estos programas a intervalos que coincidan con la vigencia prevista de las contraseñas. El descifrado de contraseñas realizado sin conexión a internet tiene un impacto mínimo o nulo en el sistema o la red, y entre sus ventajas se incluyen la validación de la política de contraseñas de la organización y la verificación de su cumplimiento.

5.2 Pruebas de penetración

Las pruebas de penetración son pruebas de seguridad en las que los evaluadores simulan ataques reales para identificar métodos que permitan eludir las medidas de seguridad de una aplicación, sistema o red. A menudo implican lanzar ataques reales contra sistemas y datos reales utilizando herramientas y técnicas comunes entre los atacantes. La mayoría de las pruebas de penetración consisten en buscar combinaciones de vulnerabilidades en uno o más sistemas que permitan obtener un acceso mayor que el que se podría lograr con una sola vulnerabilidad. Las pruebas de penetración también pueden ser útiles para determinar:

¿Qué tan bien tolera el sistema los patrones de ataque del mundo real?

El nivel de sofisticación que probablemente necesite un atacante para comprometer con éxito el sistema.

Medidas adicionales que podrían mitigar las amenazas contra el sistema

La capacidad de los defensores para detectar ataques y responder adecuadamente.

Las pruebas de penetración pueden ser invaluables, pero requieren mucho trabajo y gran experiencia para minimizar el riesgo para los sistemas objetivo. Los sistemas pueden dañarse o quedar inoperativos durante las pruebas, aunque la organización se beneficia al saber cómo un intruso podría inutilizar un sistema. Si bien los expertos en pruebas de penetración pueden mitigar este riesgo, nunca se puede eliminar por completo. Las pruebas de penetración deben realizarse solo después de una cuidadosa consideración, notificación y planificación.

Las pruebas de penetración suelen incluir métodos de ataque no técnicos. Por ejemplo, un pentester podría vulnerar los controles y procedimientos de seguridad física para conectarse a una red, robar equipos, capturar información confidencial (posiblemente mediante la instalación de registradores de pulsaciones de teclado) o interrumpir las comunicaciones. Se debe tener precaución al realizar pruebas de seguridad física: los guardias de seguridad deben saber cómo verificar la legitimidad de la actividad del pentester, por ejemplo, mediante un contacto o documentación. Otro método de ataque no técnico es la ingeniería social, como hacerse pasar por un agente de soporte técnico y llamar para solicitar las contraseñas de un usuario, o llamar al soporte técnico haciéndose pasar por un usuario y solicitar el restablecimiento de una contraseña. Información adicional sobre pruebas de seguridad física, técnicas de ingeniería social y otros métodos de ataque no técnicos incluidos en las pruebas de penetración no se aborda en esta publicación.

5.2.1 Fases de las pruebas de penetración

La figura 5-1 representa las cuatro fases de las pruebas de penetración.¹⁸ En la fase de planificación, se identifican las reglas, se finaliza y documenta la aprobación de la gerencia y se establecen los objetivos de las pruebas. Esta fase sienta las bases para una prueba de penetración exitosa. En esta fase no se realiza ninguna prueba propiamente dicha.

[18] Este es un ejemplo de cómo se puede dividir el proceso de penetración en fases. Existen muchas maneras aceptables de agrupar las acciones involucradas en la realización de pruebas de penetración.

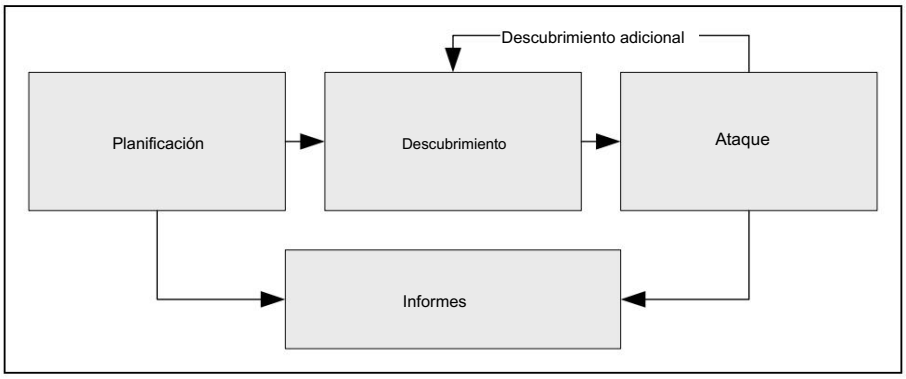

Figura 5-1. Metodología de prueba de penetración en cuatro etapas

La fase de descubrimiento de las pruebas de penetración consta de dos partes. La primera es el inicio de las pruebas propiamente dichas, y abarca la recopilación de información y el escaneo. La identificación de puertos y servicios de red, descrita en la Sección 4.2, se realiza para identificar posibles objetivos. Además de la identificación de puertos y servicios, se utilizan otras técnicas para recopilar información sobre la red objetivo.

La información sobre el nombre del host y la dirección IP se puede recopilar mediante muchos métodos, incluyendo consultas DNS, consultas InterNIC (WHOIS) y análisis de tráfico de red (generalmente solo durante pruebas internas).

Los nombres y la información de contacto de los empleados se pueden obtener buscando en los servidores web o directorios de la organización.

La información del sistema, como nombres y acciones, se puede encontrar mediante métodos como Enumeración NetBIOS (generalmente solo durante pruebas internas) y Sistema de Información de Red (NIS) (generalmente solo durante pruebas internas)

La información de la aplicación y del servicio, como los números de versión, se puede registrar mediante la captura de banners.

En algunos casos, se pueden utilizar técnicas como la búsqueda en contenedores de basura y las inspecciones físicas de las instalaciones para recopilar información adicional sobre la red objetivo, y también pueden descubrir información adicional que se utilizará durante las pruebas de penetración, como contraseñas escritas en papel.

La segunda parte de la fase de descubrimiento es el análisis de vulnerabilidades, que consiste en comparar los servicios, las aplicaciones y los sistemas operativos de los hosts escaneados con bases de datos de vulnerabilidades (un proceso automático para los escáneres de vulnerabilidades) y con el conocimiento que tienen los evaluadores sobre las vulnerabilidades. Los evaluadores humanos pueden usar sus propias bases de datos o bases de datos públicas como la Base de Datos Nacional de Vulnerabilidades (NVD). Para identificar vulnerabilidades manualmente, el Apéndice E contiene más información sobre estas bases de datos de vulnerabilidades disponibles públicamente. Los procesos manuales pueden identificar vulnerabilidades nuevas o poco comunes que los escáneres automatizados podrían pasar por alto, pero son mucho más lentos.

La ejecución de un ataque es fundamental en cualquier prueba de penetración. La figura 5-2 representa los pasos individuales de la fase de ataque: el proceso de verificación de vulnerabilidades potenciales previamente identificadas mediante el intento de explotarlas. Si un ataque tiene éxito, se verifica la vulnerabilidad y se identifican medidas de seguridad para mitigar la exposición de seguridad asociada. En muchos casos, las vulnerabilidades explotadas no otorgan acceso a la información confidencial.

[19] Los programas o scripts de explotación son herramientas especializadas para aprovechar vulnerabilidades específicas. Las mismas precauciones que se aplican a las herramientas gratuitas se aplican a los programas y scripts de explotación. Algunas bases de datos de vulnerabilidades, como Bugtraq (disponible en http://www.securityfocus.com/), proporcionan instrucciones o código para explotar muchas vulnerabilidades identificadas.

El nivel máximo de acceso potencial para un atacante. En cambio, pueden resultar en que los evaluadores aprendan más sobre la red objetivo y sus vulnerabilidades potenciales, o inducir un cambio en el estado de seguridad de la red objetivo. Algunas vulnerabilidades permiten a los evaluadores escalar sus privilegios en el sistema o la red para obtener acceso a recursos adicionales. Si esto ocurre, se requieren análisis y pruebas adicionales para determinar el nivel real de riesgo para la red, como la identificación de los tipos de información que se pueden obtener, modificar o eliminar del sistema. En caso de que un ataque a una vulnerabilidad específica resulte imposible, el evaluador debe intentar explotar otra vulnerabilidad descubierta. Si los evaluadores logran explotar una vulnerabilidad, pueden instalar más herramientas en el sistema o la red objetivo para facilitar el proceso de prueba. Estas herramientas se utilizan para obtener acceso a sistemas o recursos adicionales en la red y obtener acceso a información sobre la red o la organización. Se deben realizar pruebas y análisis en múltiples sistemas durante una prueba de penetración para determinar el nivel de acceso que un adversario podría obtener. Este proceso se representa en el ciclo de retroalimentación de la Figura 5-1 entre la fase de ataque y la fase de descubrimiento de una prueba de penetración.

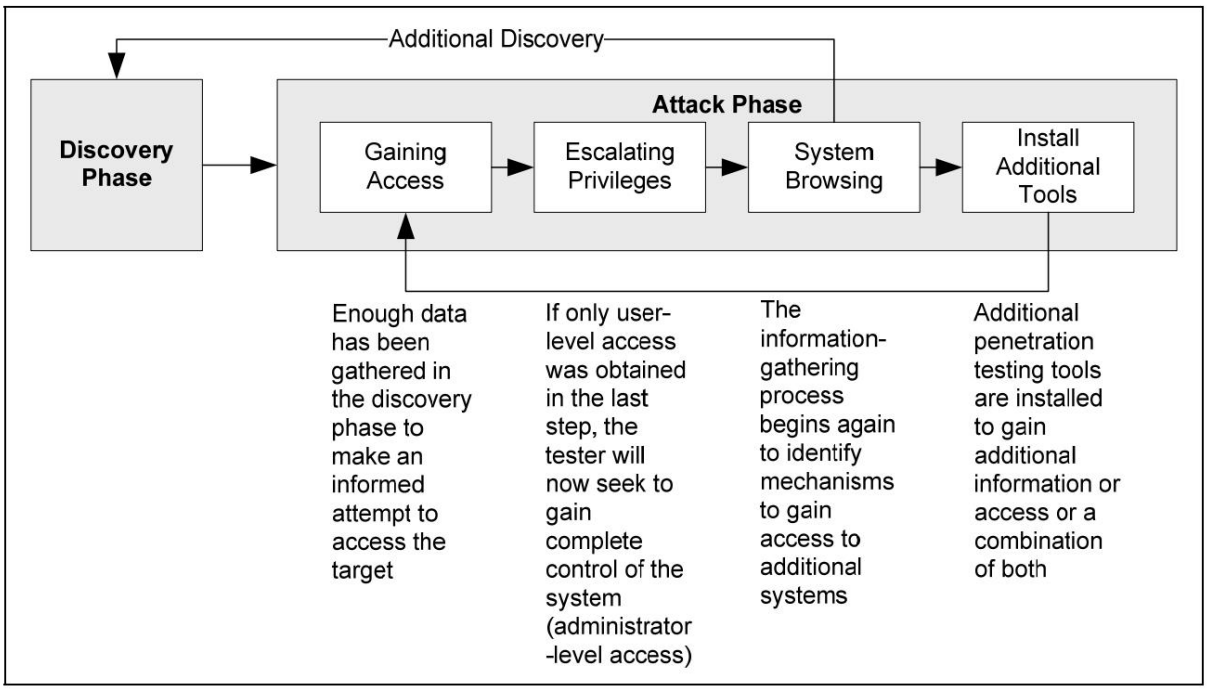

Figura 5-2. Pasos de la fase de ataque con retorno a la fase de descubrimiento

Mientras que los escáneres de vulnerabilidades solo comprueban la posible existencia de una vulnerabilidad, la fase de ataque de una prueba de penetración explota dicha vulnerabilidad para confirmar su existencia. La mayoría de las vulnerabilidades explotadas en las pruebas de penetración se clasifican en las siguientes categorías:

Configuraciones erróneas. Las configuraciones de seguridad incorrectas, en particular las configuraciones predeterminadas inseguras, suelen ser fácilmente explotables.

Fallos del núcleo. El código del núcleo es el núcleo de un sistema operativo y aplica el modelo de seguridad general del sistema; por lo tanto, cualquier fallo de seguridad en el núcleo pone en peligro a todo el sistema.

Desbordamientos de búfer. Un desbordamiento de búfer se produce cuando los programas no comprueban adecuadamente que la entrada tenga la longitud correcta. Cuando esto sucede, se puede introducir código arbitrario en el sistema y ejecutarlo con los privilegios —a menudo a nivel administrativo— del programa en ejecución.

Validación de entrada insuficiente. Muchas aplicaciones no validan completamente la entrada que reciben de los usuarios. Un ejemplo es una aplicación web que inserta un valor del usuario en una consulta a la base de datos. Si el usuario introduce comandos SQL en lugar del valor solicitado, o además de este, y la aplicación web no filtra dichos comandos, la consulta podría ejecutarse con modificaciones maliciosas solicitadas por el usuario, lo que provocaría un ataque de inyección SQL.

Enlaces simbólicos. Un enlace simbólico (symlink) es un archivo que apunta a otro archivo. Los sistemas operativos incluyen programas que pueden modificar los permisos de un archivo. Si estos programas se ejecutan con privilegios elevados, un usuario podría crear enlaces simbólicos estratégicamente para engañarlos y lograr que modifiquen o listen archivos críticos del sistema.

Ataques a descriptores de archivo. Los descriptores de archivo son números que el sistema utiliza para identificar archivos en lugar de usar nombres de archivo. Cada tipo de descriptor tiene un uso específico. Cuando un programa con privilegios asigna un descriptor de archivo incorrecto, expone el archivo a posibles ataques.

Condiciones de carrera. Las condiciones de carrera pueden ocurrir mientras un programa o proceso se encuentra en modo privilegiado. Un usuario puede programar un ataque para aprovechar los privilegios elevados mientras el programa o proceso aún está en modo privilegiado.

Permisos incorrectos de archivos y directorios. Los permisos de archivos y directorios controlan el acceso asignado a usuarios y procesos. Unos permisos deficientes podrían permitir muchos tipos de ataques, incluyendo la lectura o escritura de archivos de contraseñas o la adición de hosts a la lista de hosts remotos de confianza.

La fase de elaboración de informes se desarrolla simultáneamente con las otras tres fases de la prueba de penetración (véase la figura 5-1). En la fase de planificación, se elabora el plan de evaluación (o ROE). Durante las fases de descubrimiento y ataque, se suelen mantener registros escritos y se elaboran informes periódicos para los administradores del sistema o la dirección. Al finalizar la prueba, se elabora un informe que describe las vulnerabilidades identificadas, presenta una calificación de riesgo y ofrece recomendaciones sobre cómo mitigar las debilidades detectadas.
La sección 8 analiza con más detalle las actividades posteriores a las pruebas, como la elaboración de informes.

5.2.2 Logística de pruebas de penetración

Los escenarios de pruebas de penetración deben centrarse en localizar y explotar vulnerabilidades en el diseño e implementación de una aplicación, sistema o red. Las pruebas deben reproducir los patrones de ataque más probables y dañinos, incluyendo escenarios catastróficos como acciones maliciosas por parte de los administradores. Dado que un escenario de prueba de penetración puede diseñarse para simular un ataque interno, un ataque externo o ambos, se consideran métodos de pruebas de seguridad tanto internas como externas. Si se van a realizar pruebas internas y externas, generalmente se realizan primero las externas.

Los escenarios de ataque externo simulan a un atacante con escaso o nulo conocimiento del objetivo, que opera basándose únicamente en suposiciones. Para simular un ataque externo, los evaluadores no reciben información real sobre el entorno objetivo, salvo las direcciones IP o rangos de direcciones objetivo²⁰, y realizan investigación de código abierto, recopilando información sobre los objetivos en páginas web públicas, grupos de noticias y sitios similares. Posteriormente, utilizan escáneres de puertos y de vulnerabilidades para identificar los hosts objetivo. Dado que el tráfico de los evaluadores suele pasar por un firewall, la cantidad de información obtenida del escaneo es mucho menor que si la prueba se realizara desde una perspectiva interna. Tras identificar los hosts de la red accesibles desde el exterior, los evaluadores intentan comprometer uno de ellos. Si lo consiguen, este acceso puede utilizarse para comprometer otros hosts que normalmente no son accesibles desde el exterior.

[20] Si se les proporciona una lista de direcciones IP autorizadas para usar como objetivos, los evaluadores deben verificar que todas las direcciones públicas (es decir, no las privadas ni las no enrutables) estén bajo el control de la organización antes de comenzar las pruebas. Los sitios web que proporcionan información de registro de nombres de dominio (por ejemplo, WHOIS) pueden utilizarse para determinar los propietarios de los espacios de direcciones.

fuera de la red. Las pruebas de penetración son un proceso iterativo que aprovecha el acceso mínimo para obtener un mayor acceso.

Los escenarios de infiltración simulan las acciones de un empleado malintencionado. Una prueba de penetración interna es similar a una externa, con la diferencia de que los evaluadores se encuentran en la red interna (es decir, detrás del firewall) y se les ha concedido cierto nivel de acceso a la red o a sistemas específicos. Mediante este acceso, los evaluadores intentan obtener un mayor nivel de acceso a la red y sus sistemas a través de la escalada de privilegios. Se les proporciona información de red que normalmente tendría un empleado con su nivel de acceso, aunque, según los objetivos de la prueba, podría tratarse de información que poseería un administrador de sistemas o de red.

Las pruebas de penetración son importantes para determinar la vulnerabilidad de la red de una organización y el nivel de daño que podría ocasionar una vulneración. Es fundamental tener en cuenta que, según las políticas de la organización, los evaluadores podrían tener prohibido el uso de ciertas herramientas o técnicas, o bien, su uso podría estar limitado a determinados momentos del día o días de la semana. Las pruebas de penetración también representan un alto riesgo para las redes y los sistemas de la organización, ya que emplean exploits y ataques reales contra sistemas y datos de producción. Debido a su elevado coste y su impacto potencial, realizar pruebas de penetración en la red y los sistemas de una organización anualmente podría ser suficiente. Asimismo, las pruebas de penetración pueden diseñarse para detenerse cuando el evaluador alcance un punto en el que cualquier acción adicional cause daños. Los resultados de las pruebas de penetración deben tomarse en serio y cualquier vulnerabilidad descubierta debe mitigarse. Los resultados, una vez disponibles, deben presentarse a los directivos de la organización. Las organizaciones deberían considerar la posibilidad de realizar periódicamente actividades de prueba menos laboriosas para garantizar el mantenimiento de su nivel de seguridad. Un programa bien diseñado de escaneo regular de redes y vulnerabilidades, intercalado con pruebas de penetración periódicas, puede ayudar a prevenir muchos tipos de ataques y reducir el impacto potencial de los que tengan éxito.

5.3 Ingeniería social

La ingeniería social es un intento de engañar a alguien para que revele información (por ejemplo, una contraseña) que puede usarse para atacar sistemas o redes. Se utiliza para evaluar el factor humano y el conocimiento de los usuarios sobre seguridad, y puede revelar debilidades en su comportamiento, como el incumplimiento de los procedimientos estándar. La ingeniería social puede llevarse a cabo por diversos medios, tanto analógicos (por ejemplo, conversaciones en persona o por teléfono) como digitales (por ejemplo, correo electrónico, mensajería instantánea). Una forma de ingeniería social digital es el phishing, donde los atacantes intentan robar información como números de tarjetas de crédito, números de la seguridad social, identificadores de usuario y contraseñas. El phishing utiliza correos electrónicos de apariencia auténtica para solicitar información o redirigir a los usuarios a un sitio web fraudulento para recopilarla. Otros ejemplos de ingeniería social digital incluyen la creación de correos electrónicos fraudulentos y el envío de archivos adjuntos que podrían simular la actividad de un gusano informático.

La ingeniería social puede utilizarse para atacar a personas o grupos clave dentro de la organización, como ejecutivos, o bien para un público más amplio. Se pueden identificar objetivos específicos cuando la organización conoce una amenaza existente o considera que la pérdida de información de una persona o grupo específico podría tener un impacto significativo. Por ejemplo, los ataques de phishing pueden basarse en información pública sobre personas específicas (como cargos o áreas de interés). Si los atacantes logran obtener información o acceder a ella, atacar a personas específicas puede resultar embarazoso. Es fundamental que los resultados de las pruebas de ingeniería social se utilicen para mejorar la seguridad de la organización y no para atacar a individuos en particular. Los responsables de las pruebas deben elaborar un informe final detallado que identifique tanto las tácticas exitosas como las fallidas. Este nivel de detalle ayudará a las organizaciones a adaptar sus programas de capacitación en concientización sobre seguridad.

5.4 Resumen

Cada técnica de prueba de seguridad de la información tiene sus propias ventajas y desventajas. La tabla 5-1 compara las diversas técnicas de prueba analizadas en la sección 5.

Tabla 5-1. Técnicas de validación de vulnerabilidades del objetivo

Técnica	Capacidades
Descifrado de contraseñas	• Identifica contraseñas y políticas de contraseñas débiles • Prueba
Pruebas de penetración	la seguridad utilizando las mismas metodologías y herramientas que emplean los atacantes • Verifica las vulnerabilidades • Demuestra cómo se pueden explotar las vulnerabilidades de forma iterativa para obtener un mayor acceso • Permite probar
Ingeniería social	tanto los procedimientos como el factor humano (concienciación del usuario)

Todas las técnicas y combinaciones de técnicas conllevan riesgos. Para garantizar la ejecución segura y precisa de cada técnica, los evaluadores deben poseer un conjunto de habilidades básicas específicas. La tabla 5-2 ofrece orientación sobre las habilidades mínimas necesarias para evaluar las técnicas presentadas en esta guía.

Tabla 5-2. Conocimientos, habilidades y aptitudes para las pruebas de seguridad

Técnica	Conjunto de habilidades básicas
Descifrado de contraseñas	Conocimientos sobre la creación y el almacenamiento de contraseñas seguras para sistemas operativos; capacidad para utilizar herramientas automatizadas de descifrado de contraseñas.
Pruebas de penetración	Amplio conocimiento de TCP/IP, redes y sistemas operativos; conocimiento avanzado de vulnerabilidades y exploits de redes y sistemas; conocimiento de técnicas para evadir la detección de seguridad.
Ingeniería social	Capacidad para influir y persuadir a las personas; capacidad para mantener la compostura bajo presión.

6. Planificación de la evaluación de seguridad

Una planificación adecuada es fundamental para el éxito de una evaluación de seguridad. Esta sección ofrece orientación sobre cómo crear una política de evaluación, priorizar y programar las evaluaciones, seleccionar el enfoque de evaluación apropiado y abordar las consideraciones logísticas. También proporciona recomendaciones para desarrollar un plan de evaluación y describe las consideraciones legales relacionadas con la evaluación que las organizaciones deben tener en cuenta.

6.1 Desarrollo de una política de evaluación de seguridad

Las organizaciones deben desarrollar una política de evaluación de seguridad de la información para orientar sus evaluaciones de seguridad. Esta política debe identificar los requisitos de la evaluación de seguridad y responsabilizar a las personas encargadas de garantizar que las evaluaciones cumplan con dichos requisitos. Debe abordar:

- Requisitos organizativos que deben cumplir las evaluaciones
- Funciones y responsabilidades apropiadas (como mínimo, para aquellas personas que aprueban y ejecutan las evaluaciones)
- Adhesión a la metodología establecida
- Frecuencia de evaluación
- Requisitos de documentación, como planes de evaluación y resultados de las evaluaciones.

Una vez desarrollada y aprobada por los altos cargos pertinentes, la política debe difundirse al personal correspondiente, que podría incluir las oficinas del Director de Informática (CIO), el Director de Seguridad de la Información (CISO) y el Director de Tecnología (CTO). La dirección también debe comunicar la política a cualquier tercero que vaya a realizar evaluaciones.

Se recomienda que las organizaciones revisen su política de evaluación al menos anualmente y siempre que surjan nuevos requisitos relacionados con la evaluación. Estas revisiones determinarán la vigencia de la política, abordarán las modificaciones necesarias y brindarán oportunidades para incorporar las lecciones aprendidas.

6.2 Priorización y programación de evaluaciones

Como parte de la planificación, las organizaciones deben decidir qué sistemas deben someterse a evaluaciones de seguridad técnica y con qué frecuencia deben realizarse. Esta priorización se basa en la categorización del sistema, los beneficios esperados, los requisitos de programación y las normativas aplicables cuando la evaluación es obligatoria. Un buen punto de partida es evaluar la categorización del sistema y los requisitos asociados para la evaluación de seguridad. En este sentido, se realiza una evaluación del grado de impacto del sistema (por ejemplo, bajo, moderado, alto)[21]
El estado de la evaluación de seguridad (por ejemplo, cuándo se realizó la última evaluación) es necesario para determinar un cronograma para avanzar. Por ejemplo, las organizaciones generalmente deben evaluar un sistema de alto impacto antes que uno de impacto moderado; sin embargo, un sistema de impacto moderado cuya evaluación esté vencida podría necesitar ser evaluado antes que uno de alto impacto cuya última evaluación de seguridad aún se encuentre dentro del período aceptable.

[21] La publicación FIPS PUB 199, Estándares para la Categorización de Seguridad de la Información y los Sistemas de Información Federales, proporciona estándares para determinar la categoría de seguridad de los sistemas de información de una organización, lo cual puede ser útil para establecer una clasificación de prioridad de dichos sistemas con fines de prueba. La publicación FIPS PUB 199 está disponible para su descarga en http://csrc.nist.gov/publications/PubsFIPS.html.

plazo. Como parte de la monitorización continua,22 también deben probarse constantemente varios controles de seguridad NIST SP 800-53.23

La frecuencia de las evaluaciones suele estar determinada por los requisitos de la organización para demostrar el cumplimiento de normativas o políticas específicas. Por ejemplo, la Ley Federal de Gestión de la Seguridad de la Información (FISMA) exige pruebas periódicas, en función del riesgo, que deben realizarse al menos anualmente. Las publicaciones especiales 800-53 y 800-53A del NIST ofrecen recomendaciones a las organizaciones sobre la frecuencia de las evaluaciones de seguridad. Dado que una evaluación proporciona una visión general de la seguridad en un momento dado, las organizaciones pueden optar por exigir evaluaciones más frecuentes.

Consideraciones técnicas importantes también pueden ayudar a determinar la frecuencia de las pruebas. Por ejemplo, si se cree que un sistema tiene varias debilidades, las pruebas podrían realizarse antes para confirmar la presencia de dichas debilidades, o bien, retrasarse hasta que se hayan mitigado, para confirmar que se han resuelto.
La duración de las pruebas depende del objetivo de las mismas. Otra consideración es si alguna actividad del sistema o de la red requerida por las pruebas puede afectar la funcionalidad o la seguridad del entorno.
Por ejemplo, si se va a realizar una actualización importante, las pruebas podrían retrasarse hasta que se complete. Otro ejemplo de consideración técnica es cuando una organización desea identificar dispositivos no autorizados en redes cableadas. Esto podría lograrse mediante una o más técnicas, como el descubrimiento de la red a través de la captura pasiva de paquetes o el escaneo activo, o la revisión de los datos recopilados por el software de administración de red, los sensores de detección de intrusiones u otros dispositivos que supervisan la actividad de la red de forma rutinaria. Si estos dispositivos de supervisión pueden generar alertas en cuanto se detecta un nuevo dispositivo potencialmente no autorizado en la red, es posible que no sea necesario realizar pruebas periódicas para detectar dispositivos no autorizados, ya que se estarían realizando pruebas efectivas de forma continua.

Las organizaciones también deben considerar cuidadosamente la disponibilidad de recursos. Primero se deben identificar los recursos para los sistemas de alta prioridad, tras lo cual los sistemas de menor prioridad se pueden probar con menor frecuencia y en orden descendente. Si existe una diferencia entre los recursos necesarios y los disponibles, la organización podría necesitar asignar recursos adicionales y considerar la posibilidad de reducir el alcance de sus evaluaciones planificadas. Algunos ejemplos de elementos de alcance que pueden ser relevantes incluyen:

El tamaño de lo que se está evaluando, en términos de número de componentes (por ejemplo, una sola base de datos, todos los sistemas de usuario o la arquitectura completa) y tamaño de la red (por ejemplo, red de área local [LAN] o red de área extensa [WAN], número de ubicaciones de red a las que un evaluador deberá conectarse físicamente para realizar las pruebas).

La complejidad de lo que se evalúa. Los entornos más heterogéneos generalmente requieren mayores cantidades de recursos porque se necesitan conjuntos de habilidades y herramientas más diversos.

La viabilidad de utilizar una muestra para la evaluación, junto con el tamaño y la composición de la muestra. Por ejemplo, puede ser mucho más eficiente —y casi igual de efectivo— escanear los puertos de una pequeña muestra de hosts en lugar de miles de hosts, especialmente si los hosts están administrados y configurados de manera similar.

El nivel de recursos necesarios para llevar a cabo técnicas específicas de prueba o examen. Por ejemplo, un evaluador experto podría tardar muchas horas en revisar la documentación de seguridad completa de un sistema.

---

22 La publicación especial 800-37 del NIST, « Guía para la certificación y acreditación de seguridad de los sistemas de información federales», sección 3.4, ofrece orientación sobre la fase de monitoreo continuo del proceso de acreditación. Véase http://csrc.nist.gov/publications/PubsSPs.html.

23 Las actividades de monitoreo continuo incluyen la gestión de la configuración y el control de los componentes del sistema de información, los análisis del impacto en la seguridad de los cambios en el sistema, la evaluación continua de los controles de seguridad y la elaboración de informes de estado. La publicación especial 800-53 del NIST (http://csrc.nist.gov/publications/PubsSPs.html) ofrece orientación adicional.

El nivel de interacción humana requerido. Por ejemplo, si los evaluadores van a trabajar conjuntamente con el personal de TI, esto puede servir como una forma de capacitación para dicho personal, pero probablemente aumentará el tiempo necesario para completar la evaluación en comparación con el tiempo que necesitarían los evaluadores y el personal de TI trabajando de forma independiente.

6.3 Selección y personalización de técnicas

Existen numerosos factores a considerar al determinar qué técnicas de pruebas y exámenes técnicos deben utilizarse para una evaluación específica. En primer lugar, una organización debe definir sus objetivos de evaluación, como verificar el cumplimiento de un mandato concreto, comprobar la seguridad de un sistema como parte de las actividades de certificación y acreditación (C&A), identificar vulnerabilidades explotables en un grupo de sistemas o evaluar el rendimiento del sistema de detección de intrusiones y los procedimientos de gestión de incidentes. A continuación, la organización debe seleccionar las clases de técnicas (por ejemplo, revisión, identificación y análisis de objetivos, validación de vulnerabilidades de objetivos) que se utilizarán para obtener información que respalde dichos objetivos, así como las técnicas específicas dentro de cada clase seleccionada. Para algunas técnicas de prueba, la organización también debe determinar la perspectiva de los evaluadores (por ejemplo, interna o externa, encubierta o manifiesta) y seleccionar las técnicas correspondientes.

Dado que, en la mayoría de los casos, se puede utilizar más de una técnica para cumplir un objetivo de evaluación, las organizaciones deben determinar cuáles son las más adecuadas para cada caso. Como se analizó en la sección 6.2, un factor importante a considerar son los recursos: algunas técnicas pueden resultar considerablemente más costosas que otras debido a los tipos de herramientas necesarias y la cantidad de horas de trabajo del personal requeridas. Asimismo, algunas técnicas pueden ser demasiado largas; si el plazo para realizar una evaluación es corto, quizá se necesiten técnicas menos exhaustivas o que requieran menos recursos, como realizar un escaneo de vulnerabilidades en lugar de una prueba de penetración. Las habilidades son otro factor importante en la selección de técnicas; por ejemplo, una organización podría no contar con evaluadores en su plantilla con las habilidades necesarias para utilizar ciertas técnicas especializadas.

Las organizaciones también deben considerar cuidadosamente el riesgo al seleccionar técnicas de prueba. Algunas técnicas, como las pruebas de penetración, podrían provocar la pérdida de disponibilidad del sistema o la exposición de datos confidenciales. En algunos casos, las organizaciones deben considerar si las pruebas deben realizarse en sistemas de producción o en sistemas que no sean de producción con una configuración similar, si existen sistemas alternativos disponibles, o restringir el uso de ciertas técnicas a horarios no laborables para minimizar el impacto en las operaciones. Los factores a evaluar al tomar tales decisiones incluyen:

El posible impacto en los sistemas de producción. Por ejemplo, si una técnica de prueba en particular puede provocar una denegación de servicio, probablemente debería utilizarse en un sistema que no esté en producción.

La presencia de información personal identificable (IPI) sensible. Si las pruebas pudieran exponer IPI sensible —como números de la Seguridad Social (SSN) o información de tarjetas de crédito— a personas no autorizadas, las organizaciones deberían considerar realizar las pruebas en un sistema que no sea de producción con una versión falsa de la IPI (por ejemplo, datos de prueba en lugar de IPI real).

Es importante considerar la similitud en la configuración de los sistemas de producción y de no producción. En la práctica, suelen existir inconsistencias entre los entornos de prueba y producción, lo que puede ocasionar que se pasen por alto vulnerabilidades si se utilizan sistemas de no producción.

Las organizaciones suelen emplear una combinación de técnicas para realizar una evaluación de seguridad exhaustiva, manteniendo un nivel de riesgo aceptable para sus sistemas y redes. Como se mencionó en la Sección 2, las técnicas no técnicas pueden utilizarse en lugar de las técnicas técnicas o como complemento de estas; muchas evaluaciones emplean una combinación de ambas.

Los siguientes ejemplos muestran cómo diversas técnicas técnicas pueden complementarse entre sí y cómo la selección de técnicas puede estar relacionada con la gestión de riesgos. Estos ejemplos tienen carácter ilustrativo y no constituyen combinaciones de técnicas recomendadas para las evaluaciones de las organizaciones. Cada caso es diferente, y las organizaciones deben evaluar los requisitos y objetivos de cada evaluación al determinar la combinación de técnicas adecuada.

Identificar las debilidades técnicas en la arquitectura y configuración de seguridad de un sistema, minimizando al mismo tiempo el riesgo derivado de la propia evaluación.

– Paso 1. Revisión de la documentación. Identificar las deficiencias en las políticas y procedimientos, así como los fallos en la arquitectura de seguridad.

– Paso 2. Revisión del conjunto de reglas y la configuración de seguridad. Identificar desviaciones de
Las políticas de seguridad de la organización se manifiestan en forma de arquitectura de seguridad de red del sistema y fallos de seguridad del sistema.

– Paso 3. Escaneo inalámbrico. Identificar dispositivos inalámbricos no autorizados en las proximidades del sistema y vulnerabilidades adicionales de la arquitectura de seguridad relacionadas con las redes inalámbricas utilizadas por el sistema.

– Paso 4. Descubrimiento de red y escaneo de vulnerabilidades. Identificar todos los hosts activos dentro del sistema y sus vulnerabilidades conocidas.

Identificar y validar las debilidades técnicas en la arquitectura y configuración de seguridad de un sistema; la validación incluirá intentos de explotar vulnerabilidades seleccionadas.

– Paso 1. Revisión del conjunto de reglas y la configuración de seguridad. Identificar desviaciones de
Las políticas de seguridad de la organización se manifiestan en forma de arquitectura de seguridad de red del sistema y fallos de seguridad del sistema.

– Paso 2. Descubrimiento de red y escaneo de vulnerabilidades. Identificar todos los hosts activos dentro del sistema y sus vulnerabilidades conocidas.

– Paso 3. Prueba de penetración con ingeniería social. Validar las vulnerabilidades del sistema.

Identificar y validar las debilidades técnicas en la arquitectura y configuración de seguridad de un sistema desde la perspectiva de un atacante externo; la validación incluirá el intento de explotar algunas o todas las vulnerabilidades. Evaluar la eficacia de las capacidades de auditoría de la organización frente a ataques contra el sistema.

– Paso 1. Pruebas de penetración externas. Realizar descubrimiento de red externa, escaneo de puertos, escaneo de vulnerabilidades y ataques para identificar y validar las vulnerabilidades del sistema.

– Paso 2. Revisión de registros. Revise los registros de auditoría de control de seguridad del sistema para determinar su eficacia en la captura de información relacionada con las actividades de pruebas de penetración externas.

6.4 Logística de evaluación

Abordar la logística de las evaluaciones técnicas incluye identificar todos los recursos necesarios para realizar la evaluación; el entorno desde el cual realizar las pruebas; y las herramientas de prueba de hardware y software necesarias.
Estos temas se abordan en las subsecciones siguientes.

Además de los requisitos logísticos estándar que se describen a continuación, es igualmente importante identificar los requisitos logísticos para cada prueba durante la fase de planificación. Dependiendo del alcance y de la

Dependiendo del entorno, las pruebas individuales pueden tener requisitos logísticos adicionales, como solicitar la visita de un equipo de pruebas externo, enviar el equipo a las instalaciones para realizar las pruebas y planificar viajes locales o de larga distancia. Estas necesidades deben abordarse individualmente durante el proceso de planificación.

6.4.1 Selección y habilidades del evaluador

Los evaluadores realizan exámenes y pruebas utilizando métodos y técnicas técnicas, como las descritas en esta guía. Las organizaciones deben ser cuidadosas al seleccionar a los evaluadores, ya que contar con evaluadores debidamente capacitados, experimentados y con las credenciales adecuadas reducirá los riesgos asociados a la realización de pruebas de seguridad. Dado que los evaluadores también pueden requerir acceso a información confidencial sobre la arquitectura de la red, el estado de seguridad y las vulnerabilidades, algunas organizaciones pueden exigir verificaciones de antecedentes o autorizaciones de seguridad. Asimismo, las organizaciones deben tener en cuenta posibles conflictos de interés, como el caso de que una sola persona realice una evaluación formal y sea responsable de abordar los resultados de dicha evaluación.

Muchas organizaciones cuentan con equipos internos de evaluación. Según la estructura, el tamaño, la ubicación y los recursos disponibles de la organización, estos equipos pueden estar divididos geográficamente o centralizados y desplegados en diversas sedes para realizar sus evaluaciones. Algunos equipos se centran en competencias técnicas específicas, como las pruebas de seguridad inalámbrica, mientras que otros abarcan diversas áreas de seguridad con distintos niveles de profundidad. Por ejemplo, un equipo puede incluir, entre sus miembros, personas capaces de revisar la configuración de un sistema, otras que utilizan herramientas de evaluación automatizadas para identificar vulnerabilidades conocidas y otras que pueden explotar activamente dichas vulnerabilidades para demostrar la ineficacia de las medidas de seguridad.

Los evaluadores deben poseer amplios conocimientos de seguridad y redes, incluyendo experiencia en seguridad de redes, cortafuegos, sistemas de detección de intrusiones, sistemas operativos, programación y protocolos de red (como TCP/IP). Se requiere una amplia gama de habilidades técnicas para realizar las pruebas de manera eficaz y eficiente, minimizando el riesgo. Los evaluadores también deben dominar las técnicas específicas que se implementan, como la identificación y verificación de vulnerabilidades, la configuración de seguridad, la gestión de vulnerabilidades y las pruebas de penetración. Se prefiere la experiencia operativa a la formación teórica o práctica. Permitir que personal sin experiencia o formación realice pruebas técnicas puede afectar negativamente los sistemas y redes de una organización, obstaculizando su misión y dañando la credibilidad de su oficina de gestión del programa de seguridad y de sus evaluadores. Asimismo, es beneficioso contar con un redactor técnico u otro miembro del equipo con sólidas habilidades de redacción técnica. Esto facilita la comunicación efectiva de los resultados de la evaluación, especialmente a lectores con menor conocimiento técnico.

Cuando las evaluaciones las realiza un equipo, el líder del equipo facilita el proceso, demuestra comprender el entorno y los requisitos de la organización y, si procede, facilita la comunicación entre los evaluadores y el grupo de seguridad de la organización. El líder del equipo debe seleccionarse en función de sus conocimientos técnicos generales y su experiencia con las técnicas que se emplean, así como de su conocimiento de los activos que se evalúan. Asimismo, los líderes de equipo deben poseer excelentes habilidades de comunicación, organización, planificación y resolución de conflictos.

Las habilidades de un equipo de evaluación deben estar equilibradas para ofrecer una visión integral de la seguridad de la organización. Por ejemplo, contar con un especialista en defensa perimetral es útil, pero tener un equipo completo de especialistas en defensa perimetral probablemente sea redundante, a menos que el objetivo principal de las pruebas sea determinar la seguridad del perímetro. Idealmente, el equipo se conforma según los requisitos específicos de los exámenes y pruebas que se realizan. Las características del sistema también pueden ser importantes; por ejemplo, los sistemas de control supervisorio y adquisición de datos (SCADA) tienen varios componentes únicos con los que un evaluador de seguridad tradicional podría no estar familiarizado, lo que reduce su capacidad para evaluar de forma segura y adecuada la seguridad de dichos sistemas.

En este tipo de casos, puede ser necesario contar con uno o más expertos en la materia (SME) para complementar a los evaluadores habituales. El SME puede ser un analista de seguridad y experto en sistemas con experiencia, o bien, tener conocimientos específicos del sistema que se está evaluando. En cualquier caso, los SME deben estar familiarizados con las metas, los objetivos, el enfoque y el proceso de la evaluación, y también deben participar en la planificación siempre que sea posible, ya que pueden aportar conocimientos cruciales.

Los evaluadores deben mantenerse al día sobre las nuevas tecnologías y los métodos más recientes que un adversario podría utilizar para atacarlas. Deben actualizar periódicamente sus conocimientos, reevaluar sus metodologías y técnicas de actualización según sea necesario, y actualizar sus herramientas. Por ejemplo, asistir a cursos de capacitación técnica, realizar pruebas prácticas en un entorno de prueba o investigar las vulnerabilidades y exploits más recientes son solo algunas de las actividades que los evaluadores deben realizar con regularidad. Asimismo, deben realizar pruebas técnicas prácticas en entornos operativos de forma regular para mantener y mejorar sus habilidades.

Las responsabilidades de los evaluadores incluyen:

- Informar a las partes pertinentes —como los responsables de seguridad, la dirección, los administradores de sistemas y los usuarios — sobre las actividades de evaluación de seguridad.
- Elaboración de planes de evaluación con los administradores de sistemas, el Oficial de Seguridad de Sistemas de Información (ISSO) y el CISO
- Realizar exámenes y pruebas, y recopilar todos los datos relevantes.
- Analizar los datos recopilados y elaborar recomendaciones de mitigación
- Realizar exámenes y pruebas adicionales cuando sea necesario para validar las medidas de mitigación.

En algunos casos, la contratación de terceros (por ejemplo, auditores, personal de apoyo de contratistas) para realizar la evaluación ofrece una perspectiva y un enfoque independientes que los evaluadores internos tal vez no puedan proporcionar.
Las organizaciones también pueden recurrir a terceros para obtener conocimientos especializados que no estén disponibles internamente. Si bien puede ser beneficioso obtener una perspectiva externa sobre la seguridad, otorgar acceso a personas ajenas a la organización puede introducir riesgos adicionales. Las entidades externas deben ser debidamente evaluadas para garantizar que posean las habilidades, la experiencia y la integridad necesarias, y se les debe solicitar que asuman parte del riesgo asociado con la evaluación de seguridad, ya que podrían ser responsables de los daños sufridos por la organización evaluada. Asimismo, las entidades externas deben comprender y cumplir con las políticas, los requisitos operativos y de seguridad aplicables de la organización.

Además de las mencionadas anteriormente, las responsabilidades de los evaluadores externos incluyen:

- Coordinación y comunicación con la organización que está siendo evaluada
- Asegurar que se otorgue la autorización adecuada y mantener una copia firmada del plan de evaluación para garantizar que todas las actualizaciones queden documentadas.
- Firmar y cumplir con los acuerdos de confidencialidad requeridos
- Proteger adecuadamente los datos de acuerdo con las normas de la organización, incluyendo el manejo, la transmisión, el almacenamiento y la eliminación de todos los datos recopilados y los informes resultantes.

6.4.2 Selección de ubicación

El entorno en el que operan los evaluadores varía según las técnicas utilizadas. Para muchos tipos de pruebas, los evaluadores pueden operar tanto in situ como fuera de ella, definiéndose las pruebas in situ como aquellas que se ejecutan fuera de las instalaciones.

en las instalaciones de la organización. Sin embargo, ubicar a los evaluadores fuera de las instalaciones puede hacer que la prueba sea más realista (por ejemplo, al aplicar el enfoque de pruebas encubiertas). Para los exámenes, los evaluadores generalmente se ubican en las instalaciones para que puedan acceder fácilmente a la documentación de seguridad, los registros y otra información de la organización. Para las evaluaciones realizadas por terceros, la organización deberá determinar el nivel apropiado de acceso físico (por ejemplo, sin restricciones, con acompañamiento). Para las evaluaciones técnicas realizadas desde dentro de la red, como las revisiones de la configuración de seguridad y el escaneo de vulnerabilidades, se debe proporcionar a los evaluadores acceso a la red, ya sea en las instalaciones, a través de un túnel de red privada virtual (VPN) cifrado o mediante una conexión dedicada desde un entorno de confianza, como un laboratorio de pruebas aprobado.²⁴

Los evaluadores pueden requerir diferentes niveles de acceso a la red dependiendo de las herramientas que utilicen. Algunas herramientas requieren privilegios de administrador de red o de dominio; en tal caso, las organizaciones deben crear cuentas de administrador nuevas para su uso durante las evaluaciones. Cada evaluador debe tener su propia cuenta; las cuentas de administrador no deben compartirse bajo ninguna circunstancia. Este enfoque permite a la organización supervisar estas cuentas, que se deshabilitarán o eliminarán al finalizar la evaluación.

Las evaluaciones técnicas realizadas fuera del perímetro de la red pueden llevarse a cabo siguiendo diversos escenarios, de los cuales los más comunes se describen a continuación. Los sistemas de los evaluadores pueden conectarse directamente a un dispositivo perimetral (p. ej., un enrutador de borde), lo que los mantiene dentro de los límites lógicos y físicos de la organización. Sin embargo, esta ubicación no proporciona una evaluación precisa de la postura de seguridad de la organización desde una perspectiva adversaria. También pueden realizarse pruebas externas desde un laboratorio de pruebas con una conexión a Internet independiente de la red de la organización evaluada y, si corresponde, de la organización que realiza las pruebas (p. ej., evaluadores externos que realizan las pruebas desde sus propias instalaciones).[2] Las organizaciones que realizan pruebas externas también pueden optar por alquilar un servidor y una conexión a Internet independiente. Estos servicios los ofrecen diversos proveedores, generalmente por una cuota mensual. Si se utiliza un servidor alquilado, los evaluadores deben eliminar de forma segura los datos del sistema y reconstruirlo antes de realizar una prueba de seguridad. Una vez finalizadas las pruebas, el equipo debe seguir las directrices para el manejo de datos que se indican en la sección 7.4.

Al seleccionar una ubicación para las actividades de evaluación, las organizaciones deben considerar los riesgos inherentes al uso de ubicaciones externas. Estas suelen ofrecer menor control sobre el acceso físico y lógico que las ubicaciones internas, y pueden exponer los sistemas y datos de evaluación a un mayor riesgo de vulneración. El tráfico de red entre la ubicación externa y las instalaciones de la organización también corre mayor riesgo de ser interceptado por terceros no autorizados, lo que podría revelar vulnerabilidades de seguridad detectadas durante las pruebas. Asimismo, pueden surgir problemas al realizar ciertos tipos de pruebas, como las de penetración, en redes de terceros; dichas pruebas pueden parecer maliciosas para el personal de seguridad que supervisa el uso de la red, e incluso podrían infringir las políticas de seguridad del proveedor de red.

Como se mencionó en la Sección 5, la ubicación de los sistemas de evaluación puede afectar los resultados de ciertos tipos de pruebas. Por ejemplo, si el tráfico de red del escaneo de vulnerabilidades pasa por un firewall, este podría bloquear inadvertidamente partes del tráfico e impedir la detección de ciertas vulnerabilidades. Asimismo, los sistemas de detección y prevención de intrusiones y otros controles de seguridad podrían bloquear el tráfico de red considerado malicioso, como el de ciertos tipos de pruebas. Estos problemas se agravan cuando las pruebas se ejecutan desde una ubicación externa a través de una red de terceros, en cuyo caso ni los evaluadores ni la organización tienen conocimiento ni control sobre las medidas de seguridad que interfieren con las actividades de prueba.

---

[24] Es posible que los sistemas que se están probando no estén ubicados en una red de producción, en cuyo caso puede ser necesario proporcionar al equipo de pruebas acceso a la red que no es de producción utilizada por esos sistemas.

[25] El uso de una red independiente resulta especialmente ventajoso para realizar pruebas encubiertas. Esto dificulta que el personal de seguridad identifique el origen de la actividad (es decir, las direcciones IP no están asociadas a un equipo de pruebas ni a una organización). Además, evita una denegación de servicio involuntaria contra usuarios legítimos, que podría producirse si el personal de seguridad bloqueara el acceso desde el rango de direcciones IP de los evaluadores en respuesta a la actividad de prueba.

6.4.3 Selección de herramientas y recursos técnicos

Los sistemas de información diseñados para realizar una evaluación de seguridad deben cumplir con los requisitos específicos del tipo de evaluación y sus herramientas. Por ejemplo, los sistemas para la revisión de documentos deben contar con aplicaciones para leer documentos, rastrear vulnerabilidades y generar informes. Los sistemas diseñados para ejecutar pruebas, como evaluaciones de vulnerabilidad y pruebas de penetración, son más complejos en cuanto a requisitos del sistema y herramientas de software. Los sistemas para evaluaciones técnicas pueden incluir servidores, estaciones de trabajo o portátiles. Los portátiles suelen ser utilizados por los evaluadores que se desplazan, mientras que los servidores o las estaciones de trabajo pueden utilizarse si los evaluadores se encuentran en un laboratorio de pruebas o en las instalaciones del cliente. Los evaluadores también pueden establecer una red desde la cual ejecutar las técnicas; esto permite un entorno que admite el registro centralizado de actividades y servidores dedicados a actividades que requieren mayor capacidad de procesamiento.

Los requisitos de los sistemas de prueba varían. Para minimizar la probabilidad de fallos durante una prueba, se debe utilizar un sistema capaz de gestionar los requisitos de procesamiento y memoria de todas las herramientas, sistemas operativos y máquinas virtuales (VM)²⁶. Un fallo podría obligar a repetir ese componente de la prueba, provocar la pérdida de datos y la reconstrucción de los sistemas de prueba. Los requisitos de potencia de procesamiento y memoria dependen tanto de las herramientas utilizadas como de la velocidad con la que el equipo de pruebas espera procesar ciertos componentes. Por ejemplo, el descifrado de contraseñas generalmente requiere mayor potencia de procesamiento y memoria, por lo que los equipos de prueba podrían optar por un servidor dedicado a esta tarea. Un sistema dedicado permitirá al equipo ejecutar otros objetivos de prueba durante el proceso de descifrado de contraseñas. Los requisitos de disco duro dependerán de la cantidad de datos que se espera recopilar durante la prueba. En caso de que se requiera el almacenamiento a largo plazo de los datos, se debe identificar y adquirir un método de almacenamiento adecuado (por ejemplo, un sistema independiente o un medio extraíble).

Las herramientas que utilice el equipo de pruebas variarán según el alcance de cada prueba, pero el equipo debe contar con un conjunto básico de herramientas que utilice y mantenga actualizado. Dependiendo del proyecto y la organización, un equipo puede usar una combinación de herramientas desarrolladas internamente, herramientas de código abierto y/o herramientas comerciales o gubernamentales disponibles en el mercado (GOTS). Las herramientas deben obtenerse de fuentes reconocidas. Algunas organizaciones también pueden tener herramientas específicas que requieren o recomiendan a sus equipos; por ejemplo, una organización puede adquirir una licencia para un producto que todos sus equipos de pruebas puedan usar. También existen muchas herramientas gratuitas El Apéndice A enumera las herramientas más comunes y describe su finalidad y cómo obtenerlas. Las organizaciones deben evaluar cuidadosamente cada herramienta antes de utilizarla en una prueba; este proceso puede abarcar desde la descarga de la herramienta desde un sitio web de confianza hasta la realización de una revisión exhaustiva del código para garantizar que no contenga código malicioso.

A menudo, las herramientas determinan el sistema operativo necesario para ejecutar las pruebas, incluyendo la necesidad de múltiples sistemas operativos. Los sistemas pueden configurarse de diversas maneras, incluyendo un único sistema operativo, un único sistema operativo con imágenes de máquinas virtuales y sistemas de arranque dual. Un ejemplo de sistema de arranque dual es aquel que puede arrancar con una versión de Microsoft Windows o una versión de Linux como Red Hat, Mandrake o SuSE. Un sistema de arranque dual permite al evaluador usar dos sistemas operativos desde una misma máquina, pero esto puede resultar inconveniente, ya que requiere reiniciar el sistema para alternar entre cada sistema operativo y sus herramientas.

Otra opción más popular y funcional es usar máquinas virtuales (VM). Muchas herramientas de prueba requieren un sistema operativo específico, y las VM permiten a los evaluadores usar una mayor variedad de herramientas con más facilidad, ya que les permiten cambiar de un sistema operativo a otro sin reiniciar el sistema, lo que les permite ejecutar varios sistemas operativos simultáneamente. Esto tiene varias ventajas, como el registro de eventos y la documentación.

---

[26] Una máquina virtual (VM) es un software que permite que un único equipo host ejecute uno o más sistemas operativos invitados. Estos sistemas operativos no interactúan entre sí ni tienen conocimiento unos de otros. Un monitor de máquinas virtuales es el software que controla la comunicación entre el hardware físico y las máquinas virtuales individuales.

capacidades y ejecución de pruebas simultáneas. Dado que el sistema que aloja la máquina virtual admite dos o más sistemas operativos a la vez, los sistemas de prueba que ejecutan máquinas virtuales requieren mayor potencia de procesamiento y memoria.

Los evaluadores deben tener conocimientos, experiencia y desenvolverse con soltura en el uso de todos los sistemas operativos presentes en el sistema de prueba, ya que con frecuencia se requieren modificaciones del sistema para el correcto funcionamiento de herramientas o funcionalidades específicas. Por ejemplo, si el equipo de pruebas utiliza Red Hat Linux para realizar una prueba de seguridad inalámbrica, deberá estar familiarizado con la instalación y configuración de tarjetas de red inalámbricas, puesto que los pasos para ello podrían no ser evidentes para un usuario principiante de Red Hat Linux.

Independientemente del método de instalación del sistema, las organizaciones que realizan pruebas de seguridad deben desarrollar y mantener una imagen base como referencia. Esta imagen proporciona un conjunto de herramientas estandarizado para el equipo y permite su rápida implementación. La imagen base debe incluir el sistema operativo, los controladores, las configuraciones de sistema y seguridad necesarias, las aplicaciones y las herramientas para realizar las pruebas, así como mecanismos para el registro automático de las acciones del evaluador (por ejemplo, los comandos ejecutados). Las imágenes completas del sistema suelen depender del hardware, por lo que instalar una imagen en otro sistema con hardware diferente (por ejemplo, tarjetas gráficas) requiere que el equipo de pruebas la modifique, lo cual implica conocimientos específicos y consume mucho tiempo. Las imágenes de máquinas virtuales son más versátiles y no presentan las mismas restricciones de hardware que las imágenes completas del sistema, lo que las convierte en una opción más favorable para los equipos de pruebas. Los equipos multifuncionales, como aquellos con la capacidad de realizar escaneos de redes inalámbricas, pruebas de aplicaciones, evaluaciones de vulnerabilidades y pruebas de penetración, pueden tener una sola imagen que contenga las herramientas necesarias para ejecutar todos los tipos de pruebas o varias imágenes para diferentes técnicas. Generalmente, es preferible usar una sola imagen, ya que mantener varias requiere mantenimiento adicional.

La imagen de la máquina virtual debe actualizarse periódicamente para garantizar el uso exclusivo de las herramientas y versiones más recientes. Durante este periodo de actualización, el equipo debe confirmar la funcionalidad de las herramientas e identificar, con la documentación pertinente, cualquier cambio en su funcionamiento o uso. Actualizar las herramientas que detectan vulnerabilidades (p. ej., escáneres de vulnerabilidades) antes de cada prueba ayuda a asegurar que las vulnerabilidades descubiertas recientemente se incluyan en las pruebas. Además de mantener su conjunto de herramientas actual, el equipo debe evaluarlo periódicamente para identificar las herramientas obsoletas que deben eliminarse y las nuevas que deben añadirse.

Antes de utilizar sistemas de prueba en una prueba de seguridad, el equipo de pruebas debe aplicar los parches de seguridad más recientes y habilitar únicamente los servicios necesarios para la conectividad y las pruebas. Esta recomendación se aplica a todos los sistemas operativos que se utilicen para las pruebas, incluidos los de las máquinas virtuales. El grupo de seguridad de la organización puede validar que los sistemas de prueba cumplan con los requisitos de seguridad de la organización y estén aprobados para las pruebas antes de conectarlos a la red. La validación puede realizarse mediante los mismos sistemas utilizados para las pruebas técnicas, como los análisis de vulnerabilidades. Es posible que los sistemas de prueba no cumplan con todos los requisitos de seguridad de la organización debido a los requisitos de las herramientas utilizadas para las pruebas; por ejemplo, algunos controles de seguridad pueden interferir con el funcionamiento de las herramientas al intentar detener los análisis o ataques realizados con ellas. En tales casos, los evaluadores deberán deshabilitar estos controles de seguridad cuando se utilicen las herramientas.

Los equipos itinerantes deben contar con un kit portátil que incluya sistemas, imágenes, herramientas adicionales, cables, proyectores y demás equipo necesario para realizar pruebas en otras ubicaciones. Si una organización utiliza un equipo de pruebas externo, este no debe usar los recursos de la organización a menos que sea estrictamente necesario. Si la organización no autoriza la conexión de sistemas externos a su red, el equipo de pruebas externo deberá instalar todas las herramientas necesarias en un sistema cliente autorizado o bien proporcionar un sistema con capacidad de emulación de arranque, como un CD Live.²⁷ El Apéndice A proporciona ejemplos de dos sistemas Live.

[27] Un Live CD es un entorno de sistema operativo completamente funcional que se encuentra en un CD de arranque. Esta tecnología no requiere que el usuario instale nada (por ejemplo, software, controladores, etc.) en el sistema.

Distribuciones de CD. Si las herramientas se instalan directamente en el sistema del cliente, el equipo de pruebas debe asegurarse de que tanto las herramientas como los archivos que generen se eliminen del sistema una vez finalizadas las pruebas.

6.5 Desarrollo del plan de evaluación

Un plan de evaluación proporciona estructura y rendición de cuentas al documentar las actividades previstas para la evaluación, junto con otra información relacionada. La publicación especial 800-53A del NIST (NIST SP 800-53A) ofrece información adicional sobre los planes de evaluación y aborda varios pasos que los evaluadores deben considerar al elaborar un plan.
Estos pasos son: (i) determinar el tipo de evaluación de controles de seguridad; (ii) determinar los controles de seguridad y las mejoras de control que se incluirán en la evaluación; (iii) seleccionar los procedimientos de evaluación apropiados que se utilizarán durante la evaluación en función de los controles de seguridad y las mejoras de control del plan de seguridad del sistema; (iv) adaptar los procedimientos de evaluación seleccionados al nivel de impacto del sistema de información y al entorno operativo de la organización; (v) desarrollar procedimientos de evaluación adicionales, si es necesario, para abordar otros controles de seguridad y mejoras de control; (vi) desarrollar una estrategia para aplicar el procedimiento de evaluación ampliado; (vii) optimizar los procedimientos de evaluación para reducir la duplicación de esfuerzos y proporcionar soluciones de evaluación rentables; y (vii) finalizar el plan de evaluación y obtener las aprobaciones necesarias para su ejecución.

Cada evaluación debe abordarse en un plan de evaluación, independientemente del alcance, el nivel de intrusividad o la parte que realice la prueba (es decir, interna, externa).28 Este plan establece las reglas y los límites que los evaluadores deben respetar y protege a la organización al reducir el riesgo de un incidente como una interrupción accidental del sistema o la divulgación inadvertida de información confidencial.
Los planes de evaluación también protegen al equipo de pruebas al garantizar que la dirección de la organización comprenda y apruebe el alcance, las actividades y las limitaciones de la evaluación. El desarrollo del plan de evaluación debe ser un proceso colaborativo entre los evaluadores y los miembros clave del grupo de seguridad de la organización.

El plan de evaluación debe responder a estas preguntas básicas:

¿Cuál es el alcance de la evaluación?

¿Quién está autorizado para realizar la evaluación?

¿Cuáles son los aspectos logísticos de la evaluación?

¿Cómo se deben manejar los datos confidenciales?

¿Qué debe ocurrir en caso de incidente?

El plan de evaluación debe identificar qué sistemas y redes están autorizados para ser examinados y probados. Esto se puede hacer indicando el número de sistemas y las direcciones IP o rangos de direcciones que utilizan. El plan también debe enumerar los sistemas específicos —como mínimo por dirección IP y preferiblemente también por nombre de sistema— que no están autorizados para ser examinados o probados. Por ejemplo, si la base de datos de nóminas de una organización se considera demasiado crítica para un tipo de prueba en particular, el nombre del sistema y la dirección IP deben incluirse en la lista de exclusiones del plan de evaluación. Si la organización no controla parte o la totalidad de su red, como por ejemplo si una parte de sus sistemas se encuentra alojada en la red de un tercero, el propietario de la otra red generalmente también debe dar su consentimiento por escrito al plan de evaluación. Una situación similar implica

28 Además de un plan de evaluación, puede ser útil elaborar un documento más breve (un memorándum de una o dos páginas) que los evaluadores puedan presentar a las partes interesadas de la organización (por ejemplo, usuarios o propietarios del sistema) como autorización para acceder a sistemas específicos. El documento debe describir las actividades permitidas y no permitidas, los sistemas autorizados y no autorizados, el nivel de cooperación aceptable que deben proporcionar los usuarios y un punto de contacto en el grupo de seguridad de la organización.
Puede contactarnos para obtener más información.

Sistemas compartidos por organizaciones, como un sistema que utiliza tecnología de máquinas virtuales para prestar servicios a múltiples organizaciones. Al firmar el plan de evaluación, todas las partes reconocen y aprueban la evaluación.

Además de determinar qué sistemas están autorizados para la evaluación, el plan de evaluación debe detallar el tipo y el nivel de las pruebas permitidas. Por ejemplo, si la organización desea una evaluación de vulnerabilidades, el plan debe proporcionar información sobre las actividades autorizadas en la red objetivo, como la identificación de puertos y servicios, el escaneo de vulnerabilidades, la revisión de la configuración de seguridad y el descifrado de contraseñas, con suficiente detalle para describir el tipo de prueba, el enfoque y las herramientas. Por ejemplo, si se utilizará el descifrado de contraseñas, el método para obtenerlas (p. ej., interceptación del tráfico de red o copia del archivo de contraseñas del sistema operativo) debe incluirse en el plan. El plan también debe indicar explícitamente las actividades prohibidas, como la creación y modificación de archivos, de forma que no deje lugar a interpretaciones. Si surgen dudas sobre el alcance y el nivel de autorización durante la evaluación, los evaluadores y el contacto designado por la organización deben reunirse para tratarlas.

El plan también debe abordar los detalles logísticos de la evaluación, incluyendo el horario de atención de los evaluadores; el nivel de autorización o verificación de antecedentes requerido; un plan de comunicación con información de contacto actualizada, centros de operaciones de red y seguridad, y el contacto principal de la organización para la evaluación; la ubicación física donde se realizarán las actividades de evaluación; y el equipo y las herramientas que se utilizarán. Cualquier requisito para informar a las organizaciones matrices, las fuerzas del orden y un equipo de respuesta a incidentes informáticos (CIRT) debe especificarse en el plan de evaluación.
Además, debe identificarse a la persona responsable de informar a las organizaciones sobre la evaluación de seguridad pendiente. En el caso de pruebas encubiertas o no anunciadas, el plan de evaluación también debe definir cómo se gestionará la actividad de prueba detectada y reportada por el personal de seguridad de la organización, el CIRT y otros, incluyendo los procesos de escalamiento a seguir. El objetivo principal es garantizar que la actividad de evaluación no genere informes de brechas de seguridad a terceros, como los equipos externos de respuesta a incidentes.

En el plan de evaluación se deben identificar las direcciones IP de los equipos desde los que se realizarán las actividades de evaluación para que los administradores puedan diferenciar entre pruebas de penetración, por ejemplo, y ataques maliciosos reales. Si resulta apropiado para los objetivos de la evaluación, los administradores de seguridad pueden configurar los sistemas de detección de intrusiones y otros dispositivos de monitorización de seguridad para que ignoren la actividad generada por estas direcciones IP durante las pruebas.

Los requisitos de tratamiento de datos deben abordarse en el plan de evaluación, incluyendo:

Almacenamiento de datos organizativos durante la evaluación en los sistemas de los evaluadores, incluyendo la seguridad física de los sistemas, contraseñas y cifrado de datos.

Almacenamiento de datos tras la finalización de la evaluación, para cumplir con los requisitos de almacenamiento a largo plazo o el seguimiento de vulnerabilidades.

Transmisión de datos durante o después de la evaluación a través de redes internas o externas (por ejemplo, Internet).

Eliminación de datos de los sistemas una vez concluida la evaluación; en particular, en el caso de evaluaciones de terceros que incluyan referencias a requisitos específicos establecidos por las políticas o procedimientos de la organización rectora.

Finalmente, el plan de evaluación debe proporcionar orientación específica sobre el manejo de incidentes en caso de que los evaluadores provoquen o descubran un incidente durante el transcurso de la evaluación. Esta sección del plan

Debe definirse el término «incidente» y proporcionar directrices para determinar si se ha producido o no. El plan debe identificar puntos de contacto principales y alternativos específicos para los evaluadores, generalmente el jefe y el subjefe del equipo de evaluación, y el grupo de seguridad de la organización.
Deben incluirse directrices que indiquen claramente las acciones que deben tomar tanto los evaluadores como el grupo de seguridad de la organización al determinar que se ha producido un incidente. Por ejemplo, si los evaluadores descubren un intruso o indicios de su presencia en la red, ¿deben detenerse las pruebas? En caso afirmativo, ¿cuándo pueden reanudarse y quién debe autorizarlas? El plan de evaluación debe proporcionar instrucciones precisas sobre las acciones que deben tomar los evaluadores en estas situaciones.

Algunas evaluaciones utilizan el Registro de Evaluación (ROE, por sus siglas en inglés) como complemento o sustituto del plan de evaluación. El ROE contiene la misma información que el plan de evaluación y, además, aborda las actividades de prueba que suelen estar prohibidas por la organización. Por ejemplo, algunas actividades que se realizan con frecuencia durante las pruebas de penetración, como lanzar ataques para comprometer sistemas, generalmente están prohibidas por las políticas de la organización. El ROE autoriza a los evaluadores a realizar dichas actividades como parte del proceso de evaluación. El Apéndice B proporciona una plantilla de ejemplo para un ROE.

Cada organización debe determinar cuándo deben utilizarse los planes de evaluación y/o los registros de evaluación. Asimismo, las organizaciones deben considerar la posibilidad de desarrollar planes de evaluación centrales, plantillas de registros de evaluación o borradores parciales, y exigir su uso para promover la coherencia.

6.6 Consideraciones legales

Antes de comenzar una evaluación, se debe realizar un análisis de las posibles implicaciones legales. Si bien la participación de asesores legales queda a discreción de la organización, se recomienda su intervención en pruebas intrusivas como las de penetración. Si una organización autoriza a una entidad externa a realizar una evaluación, sus departamentos legales pueden participar. Estos departamentos pueden colaborar en la revisión del plan de evaluación e incluir cláusulas de indemnización o limitación de responsabilidad en los contratos que rigen las evaluaciones de seguridad.

En particular, para los tipos de pruebas que se consideran intrusivas. El departamento jurídico también puede exigir a las entidades externas que firmen acuerdos de confidencialidad que prohíban a los evaluadores divulgar información sensible, patentada o restringida a entidades no autorizadas.

El departamento legal también debe abordar cualquier inquietud sobre privacidad que pueda tener la organización. La mayoría de las organizaciones cuentan con avisos o acuerdos de usuario firmados que informan que sus sistemas están siendo monitoreados, advirtiendo que los usuarios consienten dicho monitoreo al utilizar el sistema. Sin embargo, no todas las organizaciones cuentan con estas medidas, y el departamento legal debe abordar las posibles violaciones de privacidad antes de que comience la evaluación. Además, los datos capturados pueden incluir información confidencial que no pertenece a la organización, o datos personales de los empleados, lo que puede generar inquietudes sobre la privacidad. Los evaluadores deben ser conscientes de estos riesgos y realizar capturas de paquetes que cumplan con los requisitos establecidos por el departamento legal. Este último también puede determinar los requisitos de manejo de datos para garantizar la confidencialidad de los mismos (por ejemplo, vulnerabilidades).

6.7 Resumen

La evaluación de la seguridad de la información es una actividad compleja debido a los requisitos organizativos, la cantidad y el tipo de sistemas que la componen, las técnicas que se utilizarán y la logística asociada. Las evaluaciones de seguridad pueden simplificarse y los riesgos asociados reducirse mediante un proceso de planificación establecido y repetible. Una planificación precisa y oportuna de la evaluación de seguridad también garantiza que se consideren todos los factores necesarios para su éxito.

Las actividades principales que implica la planificación de una evaluación incluyen:

Desarrollo de una política de evaluación de seguridad. Las organizaciones deben desarrollar una política de evaluación de seguridad de la información para orientar sus evaluaciones. Esta política debe identificar los requisitos de evaluación y responsabilizar a quienes deban garantizar su cumplimiento. La política aprobada debe difundirse entre el personal pertinente y los terceros que realicen evaluaciones para la organización. Se recomienda revisarla al menos anualmente y siempre que surjan nuevos requisitos relacionados con las evaluaciones.

Priorización y programación de evaluaciones. Las organizaciones deben decidir qué sistemas deben someterse a evaluaciones y con qué frecuencia. Esta priorización se basa en la categorización del sistema, los beneficios esperados, los requisitos de programación, las normativas aplicables donde la evaluación es obligatoria y la disponibilidad de recursos. Las consideraciones técnicas también pueden ayudar a determinar la frecuencia de las evaluaciones; por ejemplo, esperar a que se corrijan las vulnerabilidades conocidas o se realice una actualización planificada del sistema antes de realizar las pruebas.

Selección y personalización de técnicas de ensayo y evaluación técnica. Existen numerosos factores que las organizaciones deben considerar al determinar qué técnicas utilizar para una evaluación específica. Entre estos factores se incluyen los objetivos de la evaluación, las clases de técnicas que permiten obtener información para respaldar dichos objetivos y las técnicas apropiadas dentro de cada clase. Algunas técnicas también requieren que la organización determine la perspectiva de los evaluadores (por ejemplo, interna o externa) para poder seleccionar las técnicas correspondientes.

Determinar la logística de la evaluación. Esto incluye identificar todos los recursos necesarios, incluido el equipo de evaluación; seleccionar los entornos y las ubicaciones desde donde realizar la evaluación; y adquirir y configurar todas las herramientas técnicas necesarias.

Elaboración del plan de evaluación. El plan de evaluación documenta las actividades previstas para la evaluación e información relevante. Debe elaborarse un plan para cada evaluación que establezca las normas y los límites que deben respetar los evaluadores. El plan debe identificar los sistemas y redes que se evaluarán, el tipo y el nivel de pruebas permitidas, los detalles logísticos de la evaluación, los requisitos de gestión de datos y las directrices para la gestión de incidentes.

Consideraciones legales. Las organizaciones deben evaluar las posibles implicaciones legales antes de iniciar una evaluación, especialmente si esta incluye pruebas intrusivas (p. ej., pruebas de penetración) o si la va a realizar una entidad externa. Los departamentos legales pueden revisar el plan de evaluación, abordar las cuestiones de privacidad y realizar otras funciones de apoyo a la planificación de la evaluación.

7. Ejecución de la evaluación de seguridad

Durante la ejecución de la evaluación de seguridad, las vulnerabilidades se identifican mediante los métodos y técnicas definidos en la fase de planificación y recogidos en el plan de evaluación o ROE. Es fundamental que la evaluación se realice conforme al plan o ROE, y el propósito de esta sección es destacar los puntos clave que los evaluadores deben tener en cuenta durante la fase de ejecución. Por ejemplo, una coordinación adecuada durante la evaluación facilita el proceso y reduce la posibilidad de riesgos asociados. También se destacan consideraciones clave como la gestión de incidentes y los retos a los que se enfrentan las organizaciones al realizar evaluaciones. Esta sección también aborda el proceso de análisis y ofrece recomendaciones para la recopilación, el almacenamiento, la transmisión y la destrucción de los datos relacionados con la evaluación.

7.1 Coordinación

A lo largo de una evaluación, es fundamental que los evaluadores se coordinen con las distintas entidades de la organización. Los requisitos de coordinación se determinan en el plan de evaluación o en el ROE y deben cumplirse en consecuencia. Una coordinación adecuada contribuye a garantizar que:

- Las partes interesadas están al tanto del cronograma de evaluación, las actividades y los posibles impactos que la evaluación pueda tener.
- La evaluación no se realiza durante las actualizaciones, la integración de nuevas tecnologías ni en otros momentos en que se altere la seguridad del sistema (por ejemplo, las pruebas se realizan durante las ventanas de mantenimiento o los períodos de baja utilización).
- Los evaluadores disponen de los niveles de acceso necesarios a las instalaciones y los sistemas, según corresponda.
- El personal pertinente, como el CIO, el CISO y el ISSO, es informado de cualquier vulnerabilidad crítica de alto impacto tan pronto como se descubre.
- En caso de incidente, se informa a las personas pertinentes (p. ej., evaluadores, equipo de respuesta a incidentes, alta dirección). Si esto ocurre, se recomienda suspender las actividades hasta que se resuelva el incidente y se autorice a los evaluadores a reanudar sus actividades de acuerdo con el plan de evaluación o las reglas de actuación. El grado de suspensión de las actividades de evaluación varía según la organización y el tipo de incidente, pero en muchos casos, las únicas actividades que se suspenden son las que involucran los sistemas directamente afectados por el incidente.

El nivel de coordinación entre los evaluadores y la organización depende principalmente del sistema y la evaluación que se realiza. Los sistemas críticos suelen requerir mayor coordinación para garantizar su disponibilidad durante todo el proceso, y las técnicas de evaluación presentan distintos niveles de riesgo para el sistema objetivo durante su ejecución. Las técnicas de revisión conllevan un riesgo mínimo; las de identificación y análisis del objetivo, un riesgo moderado; y las de validación de vulnerabilidades del objetivo, un riesgo alto. Por ejemplo, un sistema crítico sometido a pruebas de penetración generalmente requiere mayor coordinación que una revisión documental de un sistema crítico o una prueba de penetración de un sistema no crítico. Sin embargo, las organizaciones pueden encontrarse con circunstancias en las que ocurre lo contrario, y en tales casos, el nivel de coordinación debe ajustarse a los requisitos y consideraciones organizativas. Los evaluadores y otras partes interesadas, como los propietarios del sistema, deben mantenerse alerta durante la ejecución de las evaluaciones. El nivel de acceso requerido por los evaluadores también determinará la coordinación para garantizar que dispongan del acceso físico y al sistema adecuado (por ejemplo, al evaluar la amenaza interna).

Los evaluadores deben ser proactivos en su comunicación con las partes pertinentes de la organización. Esta comunicación puede mantenerse mediante reuniones periódicas de seguimiento e informes diarios o semanales. En el plan de evaluación o en el ROE se deben identificar los asistentes a las reuniones y los destinatarios de los informes, entre los que pueden figurar los evaluadores, el ISSO, el CISO y el CIO. La frecuencia de las reuniones de seguimiento y de los informes dependerá de la duración y la complejidad de la evaluación. Por ejemplo, para una prueba de penetración de un mes, se pueden celebrar reuniones de seguimiento semanales con informes diarios durante la fase de prueba activa (es decir, el periodo durante el cual se explotan los sistemas). Las reuniones y los informes deben abordar las actividades realizadas hasta la fecha, el índice de éxito, los problemas encontrados y las conclusiones críticas/remediaciones recomendadas.

7.2 Evaluación

Como se analizó en la Sección 6, el plan de evaluación o ROE proporciona pautas para llevar a cabo la evaluación. El plan o las reglas de evaluación (ROE) deben seguirse a menos que se haya obtenido un permiso específico para desviarse, normalmente por escrito, del firmante original o de la persona a cargo. Es fundamental que todos los evaluadores lean y comprendan el plan o las ROE. Se recomienda que los evaluadores revisen periódicamente el plan o las ROE durante la evaluación, especialmente en el caso de actividades que pertenezcan a la categoría de validación de vulnerabilidades objetivo.

Durante una evaluación, el equipo de respuesta a incidentes de la organización puede detectar un incidente. Este podría deberse a las acciones de los evaluadores o a un adversario real que realice un ataque mientras la evaluación está en curso. En cualquier caso, el equipo de respuesta a incidentes o la persona que descubra el incidente debe seguir los procedimientos de escalamiento habituales de la organización, y los evaluadores deben seguir las directrices establecidas en el plan de evaluación o las reglas de enfrentamiento (ROE), a menos que se les indique lo contrario. Si se detecta la presencia de un adversario durante la evaluación, debe informarse inmediatamente a la persona correspondiente y los evaluadores deben seguir el protocolo establecido en el plan de evaluación o las ROE. Se recomienda que los evaluadores suspendan la evaluación de los sistemas involucrados en el incidente mientras la organización lleva a cabo su respuesta.

Además de encontrarse con nuevos incidentes o descubrir otros ya existentes, los evaluadores pueden enfrentarse a otros desafíos técnicos, operativos y políticos durante una evaluación. Estos pueden incluir:

Resistencia. La resistencia a las evaluaciones puede provenir de diversas fuentes dentro de una organización, incluyendo administradores de sistemas y redes, así como usuarios finales. Entre las razones se encuentran el temor a perder la disponibilidad del sistema o la red, el miedo a ser reprendidos, las molestias y la resistencia al cambio. Obtener la aprobación y el apoyo de la alta dirección ayudará a resolver los problemas relacionados con la resistencia, e incorporar las evaluaciones de seguridad en la política de seguridad general de la organización contribuirá a establecer un proceso que no sorprenda a administradores ni usuarios.

Falta de realismo. Al prepararse para una evaluación, los usuarios y administradores a veces modifican la configuración para que sus sistemas sean más seguros, resistentes a ataques o cumplan mejor con las políticas y otros requisitos. Si bien esto puede considerarse positivo, los cambios realizados en estas circunstancias generalmente solo se mantienen durante la evaluación, tras la cual los sistemas vuelven a su configuración anterior. No notificar con antelación a los usuarios y administradores sobre las evaluaciones ayuda a mitigar este problema. Muchas organizaciones realizan evaluaciones ocasionales sin previo aviso para complementar las evaluaciones anunciadas.

Mitigación inmediata. Cuando se identifican vulnerabilidades de seguridad durante una evaluación, los administradores pueden querer tomar medidas inmediatas para mitigarlas y esperar que los evaluadores vuelvan a evaluar rápidamente el sistema para confirmar que los problemas se han resuelto. Si bien este deseo de una mitigación rápida es admirable, los evaluadores deben comunicar la importancia de seguir las políticas y los procedimientos de gestión de cambios de la organización.

El tiempo es un factor crucial. La evaluación de seguridad suele incorporarse al desarrollo o la implementación con poca antelación y en plazos muy ajustados, cuando en realidad debería formar parte integral del ciclo. El tiempo también supone un desafío al probar sistemas y redes críticos en producción: si las técnicas de prueba pueden provocar una pérdida de disponibilidad u otros problemas, es posible que sea necesario probarlos fuera del horario laboral. Los evaluadores suelen estar sujetos a plazos de prueba limitados, mientras que los atacantes reales no tienen tales restricciones.

Recursos. La evaluación de seguridad se enfrenta al desafío constante de obtener y mantener recursos adecuados (por ejemplo, un equipo de pruebas capacitado y hardware y software actualizados). Se sugiere que las organizaciones designen equipos de evaluación de seguridad —como portátiles y tarjetas inalámbricas — para uso exclusivo en evaluaciones.²⁹ Si se utiliza software de evaluación comercial, se debe considerar la adquisición de licencias continuas y contratos de soporte. Los evaluadores deben programar tiempo antes de que comience la evaluación para asegurarse de que todo el software de evaluación esté debidamente actualizado y con los parches de seguridad instalados. Si no se dispone de evaluadores internos o estos no cumplen con los requisitos de evaluación, puede resultar difícil encontrar evaluadores externos confiables y con experiencia. Las organizaciones deben buscar una firma con una metodología establecida, procesos comprobados, un historial de desempeño comparable y suficiente, y personal experimentado. Si una organización utiliza evaluadores internos, debe seguir reclutando y capacitando a evaluadores calificados y ofrecerles otras oportunidades desafiantes dentro de la organización donde puedan participar para evitar el agotamiento profesional.

Tecnología en constante evolución. Los evaluadores deben mantenerse al día sobre las herramientas y las técnicas de prueba. Los presupuestos deben contemplar cursos de formación y conferencias anuales donde los evaluadores puedan actualizar y refrescar sus habilidades.

Impacto Operacional. Si bien las evaluaciones se planifican para prevenir o limitar el impacto operacional, siempre existe la posibilidad de complicaciones accidentales o imprevistas. Cada prueba realizada debe registrarse con la fecha y hora, el tipo de prueba, la herramienta utilizada, los comandos, la dirección IP del equipo de prueba, etc. Se recomienda utilizar un script de registro para capturar todos los comandos y pulsaciones de teclas utilizados durante el proceso de prueba. Existen herramientas de terminal e interfaz gráfica de usuario (GUI) que pueden registrar las acciones del evaluador, y este tipo de registro también puede ayudar a refutar acusaciones de que las pruebas han afectado negativamente las operaciones y el rendimiento del sistema. Debido al riesgo de impacto operacional, se recomienda contar con un plan de respuesta a incidentes establecido durante las pruebas.

7.3 Análisis

Aunque se puede realizar algún análisis después de completar una evaluación (véase la sección 8.1), la mayor parte del análisis se lleva a cabo durante la propia evaluación. Los objetivos principales del análisis son identificar falsos positivos, categorizar las vulnerabilidades y determinar sus causas. Las herramientas automatizadas pueden generar un número significativo de hallazgos, pero estos suelen requerir validación para aislar los falsos positivos. Los evaluadores pueden validar las vulnerabilidades examinando manualmente el sistema vulnerable o utilizando una segunda herramienta automatizada y comparando los resultados. Si bien esto puede hacerse rápidamente, estas herramientas de comparación a menudo producen resultados similares, incluidos los mismos falsos positivos. El examen manual suele proporcionar resultados más precisos que la comparación de resultados de múltiples herramientas, pero también puede resultar laborioso.

Las organizaciones pueden optar por clasificar sus hallazgos según los controles de seguridad y las familias de controles de la publicación especial 800-53 del NIST, que organiza los controles en familias como respuesta a incidentes y control de acceso. Esta clasificación puede facilitar el análisis, la corrección y la documentación de vulnerabilidades.

[29] Es posible que las organizaciones deseen desconectar sus equipos de prueba dedicados de las redes cuando no se estén realizando pruebas.

Si bien es necesario identificar y resolver las vulnerabilidades individuales, identificar la causa raíz de las vulnerabilidades es clave para mejorar la postura de seguridad general de la organización, ya que la causa raíz a menudo se puede atribuir a debilidades a nivel de programa. Algunas causas raíz comunes incluyen:

Una gestión de parches insuficiente, como no aplicarlos a tiempo o no aplicarlos a todos los sistemas vulnerables.

Gestión insuficiente de amenazas, incluyendo firmas antivirus obsoletas, filtrado de spam ineficaz y conjuntos de reglas de firewall que no aplican la política de seguridad de la organización.

Falta de estándares de seguridad básicos, como configuraciones de seguridad inconsistentes en sistemas similares.

La deficiente integración de la seguridad en el ciclo de vida del desarrollo de sistemas, como la ausencia o el incumplimiento de requisitos de seguridad y las vulnerabilidades en el código de las aplicaciones desarrolladas por la organización, representan un problema.

Las deficiencias en la arquitectura de seguridad, como la integración inadecuada de las tecnologías de seguridad en la infraestructura (por ejemplo, una ubicación deficiente, una cobertura insuficiente o tecnologías obsoletas), o la mala ubicación de los sistemas que aumenta su riesgo de vulneración, constituyen deficiencias en la arquitectura de seguridad.

Procedimientos inadecuados de respuesta a incidentes, como respuestas tardías a actividades de pruebas de penetración

Formación inadecuada, tanto para los usuarios finales (por ejemplo, no reconocer los ataques de ingeniería social y phishing, despliegue de puntos de acceso inalámbricos no autorizados) como para los administradores de redes y sistemas (por ejemplo, despliegue de sistemas con seguridad deficiente, mantenimiento de seguridad deficiente).

Falta de políticas de seguridad o de su aplicación (por ejemplo, puertos abiertos, servicios activos, protocolos no seguros, hosts no autorizados, contraseñas débiles).

Un recurso útil de referencia durante la fase de análisis es la Base de Datos Nacional de Vulnerabilidades (NVD) del NIST. La NVD es una base de datos que contiene información sobre Vulnerabilidades y Exposiciones Comunes (CVE), una lista de nombres estandarizados para vulnerabilidades conocidas. La NVD clasifica las vulnerabilidades mediante el Sistema Común de Puntuación de Vulnerabilidades (CVSS) y proporciona información adicional sobre la vulnerabilidad, así como recursos adicionales para consultar recomendaciones de mitigación (por ejemplo, sitios web de proveedores).

Otro objetivo del análisis es identificar, a lo largo de la evaluación, cualquier vulnerabilidad crítica que la organización deba abordar de inmediato. Por ejemplo, si las pruebas de penetración explotan una vulnerabilidad que permite a los evaluadores obtener privilegios de administrador en un sistema crítico, estos deben notificar inmediatamente a la persona designada en el plan de evaluación o en las reglas de evaluación.

7.4 Manejo de datos

El método mediante el cual se gestionan los datos de una organización durante la evaluación es fundamental para garantizar la protección de la información confidencial, incluyendo la arquitectura del sistema, las configuraciones de seguridad y las vulnerabilidades del sistema. Las organizaciones deben asegurar la correcta documentación de los requisitos para la gestión de datos en el plan de evaluación o en las reglas de evaluación (ROE), y cumplir con sus políticas vigentes en materia de gestión de vulnerabilidades del sistema. Esta sección ofrece métodos sugeridos para recopilar, almacenar y transmitir los datos de la evaluación durante el proceso, así como para almacenarlos y eliminarlos una vez finalizada la evaluación.

[30] El sitio web del NVD es http://nvd.nist.gov/.

7.4.1 Recopilación de datos

El equipo deberá recopilar la información pertinente durante toda la evaluación. Esto incluye información sobre la arquitectura y la configuración de las redes evaluadas, así como información sobre las actividades de los evaluadores. Dado que estos datos son confidenciales, es importante manejarlos adecuadamente.
Entre los tipos de información que los evaluadores podrían recopilar se incluyen:

Datos de arquitectura y configuración. El tipo de evaluación y el resultado deseado determinarán los datos que recopile el equipo, que pueden incluir, entre otros, nombres de sistemas, direcciones IP, sistemas operativos, ubicaciones de red físicas y lógicas, configuraciones de seguridad y vulnerabilidades.

Actividades del evaluador. Los evaluadores deben llevar un registro que incluya información del sistema de evaluación y un historial detallado de sus actividades. Esto proporciona una pista de auditoría y permite a la organización distinguir entre las acciones de los evaluadores y las de los adversarios reales. El registro de actividades también puede ser útil para elaborar el informe de resultados de la evaluación.

El uso de un registrador de pulsaciones de teclas en el sistema de un evaluador puede crear un registro detallado de muchas de sus acciones, aunque no capturará los clics del ratón ni otras acciones específicas.³¹ En el caso de herramientas automatizadas, los evaluadores pueden mantener los registros de auditoría de cada herramienta utilizada. Si bien los evaluadores pueden optar por guardar la salida del registrador de pulsaciones de teclas o del registro de auditoría de la herramienta en un sistema independiente para centralizar el almacenamiento y la auditoría, una alternativa manual consiste en un registro de actividades que rastrea cada comando ejecutado por los evaluadores en la red. Este método requiere mucho tiempo por parte de los evaluadores y es susceptible a errores.
Si se utiliza un registro de actividades, este debe incluir como mínimo la siguiente información: fecha y hora, nombre del evaluador, identificador del sistema de evaluación (es decir, IP o MAC), identificador del sistema de destino (es decir, IP o MAC), herramienta utilizada, comando ejecutado y comentarios.

7.4.2 Almacenamiento de datos

Es responsabilidad de los evaluadores almacenar de forma segura los datos recopilados durante la evaluación, incluidas las vulnerabilidades, los resultados del análisis y las recomendaciones de mitigación. La divulgación inapropiada de esta información puede dañar la reputación de la organización y aumentar la probabilidad de que se explote. Como mínimo, los evaluadores deben almacenar la siguiente información para identificar, analizar e informar sobre la postura de seguridad de la organización, y proporcionar un registro de auditoría de las actividades de prueba:

Planes de evaluación y ROE

Documentación sobre la configuración de seguridad del sistema y la arquitectura de red

Resultados de herramientas automatizadas y otros hallazgos

Informe de resultados de la evaluación

Plan de acción correctiva o Plan de Acción y Hitos (POA&M).

Existen muchas opciones para almacenar información sobre las vulnerabilidades descubiertas, como conservar los resultados en el formato de salida de la herramienta utilizada o importarlos a una base de datos.32 La mayoría de las herramientas de escaneo de vulnerabilidades tienen formatos de informe que enumeran el sistema, las vulnerabilidades y la mitigación recomendada.

---

31 Un registrador de pulsaciones de teclas registra cada tecla pulsada por el usuario del sistema y la guarda en un registro. Este nivel de registro Proporciona a los evaluadores un método para rastrear cada acción en la red y permite a la organización evaluada ver con exactitud qué ejecutaron los evaluadores en la red, cuándo ocurrió y qué sistema realizó la prueba. Además, este tipo de registro proporciona a los evaluadores documentación que demuestra que no fueron la causa del mal funcionamiento o la vulneración de un sistema de red.

32 Almacenar información sobre vulnerabilidades también puede ser útil para realizar comparaciones históricas.

Si la evaluación es de alcance limitado (por ejemplo, si solo utiliza una herramienta), este enfoque puede ser aceptable. Para evaluaciones más exhaustivas, organizaciones de mayor tamaño o evaluaciones que emplean múltiples herramientas o enfoques, se puede desarrollar un método de almacenamiento más robusto y colaborativo, como una hoja de cálculo o una base de datos. Si bien su funcionalidad es limitada, una hoja de cálculo puede ser apropiada para exámenes o pruebas individuales, ya que es fácil de usar, suele ser rápida de desarrollar y puede albergar diversas herramientas que generan resultados en un formato compatible. Para exámenes o pruebas complejos con múltiples enfoques técnicos, acciones de evaluación que se repiten con frecuencia o situaciones en las que se necesita correlacionar datos fácilmente, el desarrollo de una base de datos puede resultar beneficioso.

Las organizaciones deben garantizar el almacenamiento seguro de todos los datos de evaluación confidenciales, como el plan de evaluación o las reglas de exposición (ROE), los datos de vulnerabilidades sin procesar y los informes de evaluación. En manos de un atacante, la información sobre la arquitectura de red, la configuración del sistema, los controles de seguridad y las vulnerabilidades específicas del sistema proporcionaría un plan detallado para explotar los sistemas de información de la organización. Las organizaciones pueden optar por almacenar estos datos en medios extraíbles o en un sistema de información al que se pueda acceder según sea necesario. El medio extraíble o el sistema diseñado para almacenar esta información debe estar aislado física o lógicamente de los recursos de red de uso cotidiano. El acceso a este sistema y a la información que contiene debe limitarse a las personas cuyo acceso sea necesario para el desempeño de sus funciones y responsabilidades. Asimismo, se recomienda cifrar estos datos de conformidad con la norma FIPS 140-2 para garantizar su seguridad.

Los requisitos de retención de datos para las evaluaciones de seguridad varían y pueden no estar explícitamente establecidos para una organización. En tal caso, dichos requisitos deben especificarse en el plan de evaluación o en el registro de evaluación (ROE). Mantener registros precisos de una evaluación proporciona a la organización un historial de auditoría de sus vulnerabilidades y las medidas correctivas adoptadas para mitigar los riesgos identificados. Este historial permite a las organizaciones evaluar la eficacia de su programa de seguridad de la información mediante el análisis de tendencias de métricas como el tipo de vulnerabilidad, la frecuencia de aparición, el tiempo medio de resolución, etc.

Los sistemas de evaluación —como servidores, portátiles u otros dispositivos móviles— no deben dejarse desatendidos al almacenar datos confidenciales sin las debidas medidas de seguridad físicas y lógicas. Por ejemplo, los sistemas móviles no deben dejarse en vehículos sin seguro ni a la vista en vehículos cerrados, y los dispositivos móviles en habitaciones de hotel deben asegurarse con un candado de cable, guardarse en la caja fuerte de la habitación o protegerse físicamente por otros medios. Además de estas medidas de seguridad físicas, los evaluadores deben asegurarse de que el sistema esté configurado de forma que impida que personas malintencionadas lo vulneren. Los evaluadores deben tomar las medidas apropiadas para garantizar la integridad y la confidencialidad de los datos que contiene el sistema y protegerlo, como mínimo, con una contraseña robusta; además, se sugiere que las organizaciones consideren el uso de la autenticación de dos factores.³³ Asimismo, todos los datos confidenciales del sistema deben estar cifrados³⁴ y debe utilizarse un mecanismo de autenticación independiente del sistema para restringir el acceso a la información cifrada.

7.4.3 Transmisión de datos

Puede ser necesario transmitir datos de evaluación, como configuraciones y vulnerabilidades del sistema, a través de la red o Internet, por lo que es fundamental garantizar la seguridad de dichos datos para protegerlos de posibles vulneraciones. El plan de evaluación o la regla de evaluación (ROE) debe abordar los requisitos y el proceso para la transmisión de información confidencial del sistema a través de la red o Internet. Los métodos de transmisión segura de datos incluyen el cifrado de archivos individuales que contienen información confidencial y el cifrado de las comunicaciones.

---

[33] La autenticación de dos factores proporciona seguridad adicional al requerir dos de los siguientes tres factores: algo que sabes (por ejemplo, una contraseña), algo que tienes (por ejemplo, un token de seguridad) y algo que eres (por ejemplo, un escaneo de retina).

[34] Dichos datos deben cifrarse de conformidad con FIPS 140-2 para garantizar que permanezcan seguros.

canales que utilizan cifrado compatible con FIPS (por ejemplo, VPN, protocolo Secure Sockets Layer [SSL]) y que proporcionan información a través de copias impresas o digitales entregadas o enviadas por correo.

7.4.4 Destrucción de datos

Cuando ya no se necesiten los datos de evaluación, los sistemas de evaluación, la documentación impresa y los soportes deberán eliminarse adecuadamente. La publicación NIST SP 800-88, Directrices para la eliminación de soportes35, divide la eliminación de soportes en cuatro categorías:

> Eliminación: acto de desechar soportes sin ninguna otra consideración de higienización. Esto se realiza con mayor frecuencia mediante el reciclaje de papel que contiene información no confidencial, pero también puede incluir otros soportes.
>
> Borrado seguro: un nivel de saneamiento de medios que protege la confidencialidad de la información frente a un ataque de teclado avanzado. La simple eliminación de elementos no es suficiente para el borrado seguro. Este debe impedir que la información sea recuperada por utilidades de recuperación de datos, discos o archivos, y debe ser resistente a los intentos de recuperación mediante pulsaciones de teclas ejecutadas desde dispositivos de entrada estándar y herramientas de recuperación de datos. La sobreescritura es un ejemplo de un método aceptable para el borrado seguro de medios.
>
> Purga: proceso de saneamiento de medios que protege la confidencialidad de la información frente a ataques de laboratorio.³⁶ En algunos medios, el borrado no es suficiente para la purga. Como alternativas, se puede ejecutar el comando de borrado seguro del firmware (solo para unidades ATA) y desmagnetizar.³⁷
>
> Destrucción: obliteración física del soporte para que deje de ser utilizable para su propósito original y los datos que contiene sean irrecuperables. La destrucción física puede realizarse mediante diversos métodos, como la desintegración, la incineración, la pulverización, el triturado y la fusión.

Las organizaciones deben contar con una política sobre sus requisitos de desinfección para los sistemas de evaluación. La publicación especial 800-88 del NIST (NIST SP 800-88) presenta un diagrama de flujo de decisiones para ayudar a las organizaciones a determinar qué método de desinfección es el más adecuado para sus circunstancias. Un plan de evaluación o un registro de evidencia (ROE) también puede especificar los requisitos de destrucción para pruebas específicas.

Los evaluadores externos deben asegurarse de comprender los requisitos de la organización en materia de desinfección, ya que las políticas pueden diferir entre organizaciones y posiblemente entre divisiones dentro de la misma organización.
Por ejemplo, algunas organizaciones prohíben que los evaluadores externos tengan acceso a los datos de la evaluación una vez presentados sus informes finales. En tales casos, una persona cualificada de la organización evaluada debe verificar que se hayan implementado las medidas de saneamiento adecuadas.

---

35 La publicación NIST SP 800-88 está disponible en http://csrc.nist.gov/publications/PubsSPs.html.

36 Un ataque de laboratorio implicaría a un atacante con los recursos y el conocimiento necesarios para utilizar sistemas no estándar e intentar recuperar datos de soportes fuera del entorno operativo normal. Este tipo de ataque requiere el uso de equipos de procesamiento de señales y personal especializado.

37 La desmagnetización consiste en exponer el medio magnético a un campo magnético intenso para alterar los dominios magnéticos registrados.

8. Actividades posteriores a la prueba

Tras la fase de ejecución —cuyos resultados se expresan en términos de vulnerabilidades— la organización debe tomar medidas para abordar las vulnerabilidades identificadas. Esta sección presenta maneras en que las organizaciones pueden traducir sus hallazgos en acciones que mejoren la seguridad. Primero, se debe realizar un análisis final de los hallazgos y desarrollar acciones de mitigación. Segundo, se debe elaborar un informe que presente las recomendaciones. Por último, se deben llevar a cabo las actividades de mitigación. Muchas de las acciones presentadas en esta sección pueden realizarse fuera del proceso de pruebas en sí; por ejemplo, como parte de una evaluación de riesgos que utilice los resultados de las pruebas.

8.1 Recomendaciones de mitigación

Como se describe en la Sección 7.3, la mayor parte del análisis se realiza durante el proceso de pruebas. El análisis final, como la elaboración de conclusiones generales, suele tener lugar una vez completadas todas las actividades de prueba e implica el desarrollo de recomendaciones de mitigación. Si bien la identificación y categorización de vulnerabilidades es importante, una prueba de seguridad resulta mucho más valiosa si, además, da como resultado el desarrollo e implementación de una estrategia de mitigación. Para cada hallazgo, se deben desarrollar recomendaciones de mitigación, incluyendo el resultado del análisis de la causa raíz. Estas recomendaciones pueden ser tanto técnicas (por ejemplo, la aplicación de un parche específico) como no técnicas, que abordan los procesos de la organización (por ejemplo, la actualización del proceso de gestión de parches). Algunos ejemplos de acciones de mitigación incluyen modificaciones de políticas, procesos y procedimientos; cambios en la arquitectura de seguridad; la implementación de nuevas tecnologías de seguridad; y la implementación de parches para el sistema operativo y las aplicaciones.

La publicación especial 800-53 del NIST (NIST SP 800-53) propone recomendaciones de mitigación para cada control de seguridad. Las organizaciones deben comparar las posibles medidas de mitigación con los requisitos operativos para determinar las que mejor equilibren la funcionalidad y la seguridad. La sección 8.3 aborda la implementación de las recomendaciones de mitigación.

8.2 Informes

Una vez finalizado el análisis, se generará un informe que identifique las vulnerabilidades del sistema, la red y la organización, así como las acciones de mitigación recomendadas. Los resultados de las pruebas de seguridad pueden utilizarse de las siguientes maneras:

- Como punto de referencia para la acción correctiva
- Al definir las actividades de mitigación para abordar las vulnerabilidades identificadas
- Como referencia para evaluar el progreso de una organización en el cumplimiento de los requisitos de seguridad
- Para evaluar el estado de implementación de los requisitos de seguridad del sistema
- Realizar un análisis de costo-beneficio para las mejoras en la seguridad del sistema.
- Para mejorar otras actividades del ciclo de vida, como las evaluaciones de riesgos, la certificación y acreditación, y los esfuerzos de mejora de procesos.
- Para cumplir con los requisitos de información, como los de FISMA.

Los resultados de las pruebas de seguridad deben documentarse y ponerse a disposición del personal pertinente, que puede incluir al CIO, CISO y ISSO, así como a los responsables de programa o propietarios del sistema correspondientes. Dado que un informe puede estar dirigido a varios destinatarios, es posible que se requieran varios formatos para garantizar que todos sean atendidos adecuadamente. Por ejemplo, las organizaciones que elaboran informes para el cumplimiento de FISMA deben

Cumplir con los requisitos de FISMA, como la presentación de informes sobre los resultados de las evaluaciones, el cumplimiento de las normas NIST, las deficiencias significativas y las actividades de remediación planificadas. Los informes que permanecerán dentro de la organización pueden adaptarse a las audiencias pertinentes, como la gestión de programas, la gestión de la información, los ingenieros de seguridad, la gestión de la configuración o el personal técnico. Los informes internos deben incluir la metodología de pruebas, los resultados de las pruebas, el análisis y el Plan de Acción y Metodología (POA&M). Un POA&M garantizará que las vulnerabilidades individuales se aborden con acciones específicas, medibles, alcanzables, realistas y tangibles.

8.3 Remediación/Mitigación

El Plan de Acción y Mitigación (POA&M) proporciona a la oficina de gestión del programa los detalles y las acciones necesarias para mitigar el riesgo de manera adecuada y aceptable. Como complemento del POA&M, las organizaciones pueden considerar el desarrollo de una estrategia o un proceso para la implementación del plan. Durante el proceso de implementación de la remediación, las organizaciones deben seguir al menos los cuatro pasos que se describen a continuación; estos pasos proporcionarán coherencia y estructura al personal de seguridad y a los gestores del programa.

El primer paso del proceso consiste en probar la recomendación de remediación. Antes de implementar modificaciones técnicas en un activo de producción, se deben realizar pruebas en sistemas de prueba en un entorno que replique la red en la que se implementaría la medida de mitigación. Por ejemplo, antes de su distribución a toda la empresa, se deben instalar parches en sistemas comparables del entorno de prueba para determinar si existen consecuencias negativas. Estas pruebas reducen significativamente, aunque no eliminan, el riesgo de que un sistema reaccione de forma adversa a una modificación técnica.

En segundo lugar, el Plan de Acción y Mitigación (POA&M) debe coordinarse a través del comité de control de configuración o de gestión de la configuración de la organización, ya que probablemente proponga cambios en los sistemas, redes, políticas o procesos existentes. Comunicar los cambios del POA&M antes de su implementación y al finalizarla garantiza que las personas pertinentes estén al tanto de los cambios pendientes y su impacto en el entorno, la misión y las operaciones. Como mínimo, se debe contactar al director del programa o al propietario del sistema antes de ejecutar cualquier acción del POA&M, y este debe aprobar las acciones de mitigación planificadas antes de su implementación.

Obtener la aprobación de la gerencia puede ser un reto. Conviene identificar el motivo de su necesidad (es decir, si se debe a políticas o tecnología) y el impacto positivo que se logrará con la medida de mitigación (por ejemplo, mayor seguridad o cumplimiento normativo). Un análisis de costo-beneficio también puede proporcionar a los gerentes un análisis cuantitativo del aumento en los ahorros que se obtendrán al implementar los elementos del Plan de Acción y Mitigación (POA&M). Otros beneficios que se pueden comunicar a la alta gerencia incluyen una menor exposición a riesgos, un mayor control de los activos, una reducción de vulnerabilidades, un enfoque proactivo de la seguridad y el mantenimiento del cumplimiento normativo.

En tercer lugar, se implementan y verifican las medidas de mitigación para garantizar su correcta y adecuada aplicación. La verificación puede realizarse mediante una auditoría del sistema, la repetición de pruebas del sistema y sus componentes, y la documentación que responsabiliza al personal. Una auditoría del sistema proporciona una verificación técnica de los cambios implementados y puede ser realizada por personal de seguridad in situ o por un equipo externo de pruebas de seguridad. El equipo auditor puede utilizar la estrategia de mitigación como lista de verificación para asegurar que cada acción se haya completado; además, la repetición de pruebas del sistema validará que las medidas de mitigación se hayan llevado a cabo. Es importante destacar que el equipo de pruebas solo podrá verificar la implementación si se realiza una réplica exacta de la prueba original. A medida que la tecnología evoluciona,

[38] La publicación especial 800-37 del NIST señala que un Plan de Acción y Medidas (POA&M) «describe las medidas que se han implementado o planificado para: (i) corregir cualquier deficiencia detectada durante la evaluación de los controles de seguridad; y (ii) reducir o eliminar las vulnerabilidades conocidas en el sistema». Sistema de información. El documento de plan de acciones e hitos identifica: (i) las tareas que deben realizarse; (ii) los recursos necesarios para llevar a cabo los elementos del plan; (iii) los hitos para el cumplimiento de las tareas; y (iv) las fechas de finalización previstas para los hitos.

Es posible que se descubran vulnerabilidades adicionales durante las pruebas de seguridad posteriores. Una organización también puede optar por verificar la implementación de la estrategia de mitigación mediante métodos no técnicos, como la documentación. Por ejemplo, puede ser apropiado y rentable exigir al personal de seguridad responsable de la implementación de la estrategia de mitigación que firme un documento que describa todas las acciones realizadas. Si bien este método es más rentable a corto plazo para una organización, existen riesgos al no verificar técnicamente que los cambios se hayan implementado.

Por último, como parte de la estrategia de implementación, es importante actualizar continuamente los Planes de Acción y Gestión (POA&M) para identificar las actividades que se han completado, se han completado parcialmente o están pendientes de acción por parte de otra persona o sistema. Garantizar que el POA&M esté integrado en el proceso de gestión de la configuración de la organización facilitará el seguimiento y la gestión centralizados de los cambios en sistemas, políticas, procesos y procedimientos, además de proporcionar un mecanismo de supervisión que garantizará el cumplimiento de los requisitos normativos.

Apéndice A: Distribuciones de CD Live para pruebas de seguridad

Los CD de distribución en vivo, centrados en pruebas de seguridad, están disponibles gratuitamente para el público y proporcionan a los evaluadores de seguridad un sistema operativo de distribución en vivo que incluye herramientas para dichas pruebas.³⁹ La distribución del sistema operativo se carga en un CD-ROM, una unidad USB u otro dispositivo periférico. No se instala en el sistema, sino que se ejecuta directamente desde el dispositivo en el que se carga; de ahí su denominación como distribución «en vivo». Dos ejemplos de estas distribuciones son BackTrack y Knoppix Security Tool Distribution (STD).

BackTrack40 incluye una colección de más de 300 herramientas de seguridad para el descubrimiento de redes, escaneo y análisis de tráfico, descifrado de contraseñas, pruebas de acceso remoto, pruebas de Bluetooth, análisis forense informático y pruebas de penetración. Ofrece modularidad para el usuario, lo que significa que este puede personalizar la distribución para incluir scripts personales o herramientas adicionales. BackTrack también incluye herramientas para analizar protocolos de Voz sobre Internet (VoIP), como el Protocolo de Inicio de Sesión (SIP); herramientas como Cisco Global Exploiter (CGE) y Cisco Torch, diseñadas específicamente para sistemas Cisco; y Metasploit, una herramienta de evaluación de vulnerabilidades. Consciente de la creciente importancia de las pruebas de seguridad de aplicaciones, también incluye herramientas como Peach, Fuzzer y la herramienta Java Paros Proxy. La Tabla A-1 muestra una muestra de las herramientas disponibles en BackTrack. [1]

Tabla A-1. Ejemplo del kit de herramientas BackTrack

Técnica de prueba de seguridad	Herramienta de prueba de seguridad
Revisar	
Análisis de red	Dsniff, Ettercap, Kismet, Mailsnarf, Msgsnarf, Ntop, Phoss, SinFP, SMB Sniffer y Wireshark
Comprobación de la integridad de los archivos	Autopsy, Foremost, RootkitHunter y Sleuthkit
Identificación y análisis de objetivos	
Pruebas de seguridad de aplicaciones	CIRT Fuzzer, Fuzzer 1.2, NetSed, Paros Proxy, Peach Autonomous System
Descubrimiento de redes	Scanner, Ettercap, Firewalk, Netdiscover, Netenum, Netmask, Nmap, P0f, Tctrace y Umit
Puerto de red y servicio Identificación	Amap, AutoScan, Netdiscover, Nmap, P0f, Umit y UnicornScan
Escaneo de vulnerabilidades	Firewalk, GFI LANguard, Hydra, Metasploit, Nmap, Paros Proxy, Snort y SuperScan
Escaneo inalámbrico	Airsnarf, Airsnort, BdAddr, Bluesnarfer, Btscanner, FakeAP, GFI LANguard, Kismet y WifiTAP
Validación de vulnerabilidades del objetivo	
Descifrado de contraseñas	Hydra, John el Destripador, RainbowCrack, Rcrack, SIPcrack, SIPdump, TFTP-Brute, THC PPTP, VNCrack y WebCrack
Pruebas de acceso remoto	IKEProbe, IKE-Scan, PSK-Crack y VNC_bypauth
Pruebas de penetración	Driftnet, Dsniff, Ettercap, Kismet, Metasploit, Nmap, Ntop, SinFP, SMB Sniffer y Wireshark

39 Estos conjuntos de herramientas no incluyen necesariamente todas las herramientas necesarias para una prueba en particular; en muchos casos, será necesario complementarlos con herramientas adicionales.

40 BackTrack se deriva de dos distribuciones Linux Live independientes centradas en la seguridad: WHAX y Auditor Security Collection. Ambas gozaban de popularidad por su gran cantidad de herramientas de seguridad y su facilidad de uso. Poco después de que los creadores de cada distribución comenzaran a colaborar, lanzaron la primera versión no beta, renombrada BackTrack, en mayo de 2006. BackTrack se convirtió rápidamente en una de las herramientas favoritas entre los profesionales de seguridad y aún lo sigue siendo. En esta publicación se hace referencia a la versión 3.0 de BackTrack.

41 Muchas de las herramientas enumeradas en las tablas A-1 y A-2 podrían enumerarse para técnicas adicionales, pero por brevedad no se hace.

Knoppix STD, una distribución Linux Live antigua y un conjunto de herramientas de seguridad de código abierto, se basa en Knoppix Linux. Fue creada por un profesional de la seguridad para facilitar la enseñanza de técnicas de seguridad. Knoppix STD se lanzó por primera vez en mayo de 2004 como Knoppix-STD 0.1 y no se ha actualizado desde entonces. La falta de una versión más reciente se debe a que su creador abandonó el proyecto. En esta publicación se hace referencia a la versión 0.1. Antes de BackTrack, Knoppix STD era el conjunto de herramientas de seguridad de referencia y sigue siendo ampliamente utilizado.

Al igual que BackTrack, Knoppix STD permite el descubrimiento de redes, la identificación de puertos y servicios, el análisis de tráfico de red, el descifrado de contraseñas, el análisis forense y las pruebas de acceso remoto. Si bien existen algunas similitudes entre las distribuciones, también hay diferencias. Knoppix incluye herramientas que BackTrack no tiene, como Netcat y Nessus; abarca áreas tecnológicas como la criptografía; y ofrece más herramientas para el análisis forense informático y el análisis de tráfico. No incluye Metasploit y, en comparación con BackTrack, presenta limitaciones en cuanto a herramientas de seguridad inalámbrica. La tabla A-2 muestra una muestra de las herramientas disponibles en la distribución Knoppix STD.

Tabla A-2. Ejemplo del kit de herramientas Knoppix STD

Técnica de prueba de seguridad	Herramienta de prueba de seguridad
Revisar	
Análisis de red	Dsniff, Ettercap, Ethereal, Filesnarf, Kismet, Mailsnarf, Msgsnarf, Ngrep, Ntop, TCPdump y Webspy
Comprobación de la integridad de los archivos	Autopsia, Biew, Bsed, Coreografía, Foremost, Hashdig, Rifiuti y Kit de detective
Identificación y análisis de objetivos	
Pruebas de seguridad de aplicaciones	NetSed
Descubrimiento de redes	Cryptcat, Ettercap, Firewalk, Netcat, Nmap y P0f
Identificación de puerto de red y servicio	Amap, Netcat, Nmap y P0f
Escaneo de vulnerabilidades	Exodus, Firewalk, Nmap y Snort
Escaneo inalámbrico	Airsnarf, Airsnort, GPSdrive, Kismet y MACchanger
Validación de vulnerabilidades del objetivo	
Descifrado de contraseñas	Allwords2, chntpw, Cisilia, Djohn, Hydra, Juan el Destripador y Rcrack
Pruebas de acceso remoto	Servidor Apache, IKE-Scan, Net-SNMP, SSHD, TFTPD y VNC Servidor
Pruebas de penetración	Driftnet, Dsniff, Ethereal, Ettercap, Kismet, Nessus, Netcat, Ngrep, Nmap, Ntop y TCPdump

Apéndice B—Plantilla de reglas de participación

Esta plantilla proporciona a las organizaciones un punto de partida para desarrollar su ROE.[42] Las organizaciones individuales pueden encontrar necesario incluir información para complementar lo que se describe aquí.

1. Introducción

1.1. Objetivo

Identifica el propósito del documento, así como la organización que se está probando, el grupo que realiza la prueba (o, si se trata de una entidad externa, la organización contratada para realizar la prueba) y el propósito de la prueba de seguridad.

1.2. Alcance

Identifica los límites de las pruebas en términos de acciones y resultados esperados.

1.3. Supuestos y limitaciones

Identifica cualquier supuesto realizado por la organización y el equipo de pruebas. Estos pueden estar relacionados con cualquier aspecto de la prueba, incluyendo el equipo de pruebas, la instalación de salvaguardas apropiadas para los sistemas de prueba, etc.

1.4. riesgos

Existen riesgos inherentes al realizar pruebas de seguridad de la información, especialmente en el caso de pruebas intrusivas. Esta sección debe identificar estos riesgos, así como las técnicas de mitigación y las acciones que debe emplear el equipo de pruebas para reducirlos.

1.5. Estructura del documento

Describe la estructura del ROE y el contenido de cada sección.

2. Logística

2.1. Personal

Debe identificar por nombre a todo el personal asignado a la tarea de pruebas de seguridad, así como al personal clave de la organización evaluada. Debe incluir una tabla con todos los contactos del equipo de pruebas, el personal directivo pertinente y el equipo de respuesta ante incidentes. Si corresponde, también se deben proporcionar las autorizaciones de seguridad o información similar sobre la verificación de antecedentes.

2.2. Calendario de pruebas

Detalla el cronograma de pruebas e incluye información como las pruebas críticas y los hitos. Esta sección también debe indicar el horario en el que se realizarán las pruebas; por ejemplo, puede ser conveniente realizar las pruebas técnicas de un sitio operativo durante la noche en lugar de durante las horas punta.

[42] La estructura de esta plantilla tiene carácter meramente ilustrativo. Las organizaciones deben organizar sus registros de entidades de la manera que consideren oportuna.

2.3. Sitio de prueba

Identifica la(s) ubicación(es) desde la(s) que se autorizan las pruebas. Si las pruebas se realizarán en las instalaciones de la organización, se debe definir el acceso a los edificios y equipos. El acceso físico debe contemplar requisitos como credenciales, acompañamiento y personal de seguridad con el que los evaluadores puedan interactuar. El acceso a los equipos debe especificar el nivel de acceso (usuario o administrador) a los sistemas y/o la red, así como el acceso físico a las salas de servidores o a los racks específicos que contienen. También se deben identificar las áreas a las que el equipo de pruebas no tendrá acceso.

Si las pruebas se realizarán desde una ubicación remota, como una granja de servidores o un laboratorio de pruebas alquilado, en esta sección se deben incluir los detalles de la arquitectura del sitio de pruebas.

2.4. Equipos de prueba

Identifica el equipo que el equipo de pruebas utilizará para realizar las pruebas de seguridad de la información. Esta sección también debe especificar el método para diferenciar entre los sistemas de la organización y los sistemas que realizan las pruebas; por ejemplo, si los sistemas del equipo de pruebas se identifican por su dirección MAC, el seguimiento de los sistemas de prueba podría realizarse mediante software de detección de red. Además del hardware, deben identificarse las herramientas autorizadas para su uso en la red. Asimismo, sería conveniente incluir una descripción de cada herramienta en un apéndice.

3. Estrategia de comunicación

3.1. Comunicación general

Se analizan la frecuencia y los métodos de comunicación. Por ejemplo, se identifican el calendario de reuniones, las ubicaciones y la información sobre las conferencias telefónicas, si procede.

3.2. Gestión y respuesta ante incidentes

Esta sección es fundamental en caso de que ocurra un incidente en la red mientras se realizan las pruebas.
Deben proporcionarse los criterios para detener las pruebas de seguridad de la información, así como los detalles del plan de acción del equipo de pruebas en caso de que un procedimiento de prueba afecte negativamente la red o un adversario ataque la organización mientras se realizan las pruebas. El árbol de llamadas/cadena de mando para la respuesta a incidentes de la organización debe proporcionarse en un formato de referencia rápida. También debe proporcionarse un proceso para reintegrar al equipo de pruebas y reanudar las pruebas.

4. Sistema/Red de destino

Identifica los sistemas y/o redes que se probarán a lo largo del proceso de pruebas de seguridad de la información.
La información debe incluir las direcciones IP autorizadas y no autorizadas, u otros identificadores distintivos, si procede, para los sistemas (servidores, estaciones de trabajo, cortafuegos, enrutadores, etc.), los sistemas operativos y las aplicaciones que se vayan a probar. También es fundamental identificar cualquier sistema no autorizado para las pruebas; a esto se le denomina «lista de exclusión».

5. Ejecución de pruebas

Esta sección se centra en el tipo y alcance de las pruebas, pero debe detallar las actividades permitidas y no permitidas e incluir una descripción de la metodología de pruebas de seguridad de la información. De ser necesario, se debe elaborar un plan de evaluación que complemente las Reglas de Entendimiento (ROE); este plan puede presentarse como un apéndice o un documento aparte.

5.1. Componentes de prueba no técnicos

Identifica las actividades de prueba no técnicas que se llevarán a cabo e incluye información para ayudar a determinar los tipos de políticas, procedimientos y otros documentos que deben revisarse. Si se van a realizar entrevistas o inspecciones de las instalaciones, se deben establecer directrices para la aprobación previa de la lista de entrevistados y las preguntas. Si la seguridad física de los sistemas de información forma parte del alcance de las pruebas, se deben determinar los procedimientos y generar un formulario —con las firmas y la información de contacto correspondientes— para que el equipo de pruebas lo muestre a las autoridades o al personal de seguridad del lugar en caso de que se les solicite información.

5.2. Componentes de prueba técnica

Incluye el tipo de pruebas técnicas que se realizarán (p. ej., escaneo de red, descubrimiento, pruebas de penetración); indica si se autoriza la instalación, creación, modificación o ejecución de archivos para facilitar las pruebas; y explica las acciones necesarias para dichos archivos una vez finalizadas las pruebas. Cualquier información adicional sobre las pruebas técnicas de los sistemas y redes de la organización también debe incluirse en esta sección. Se debe proporcionar información detallada sobre las actividades que se realizarán en la red objetivo para garantizar que todas las partes estén al tanto de lo que está autorizado y de lo que cabe esperar como resultado de las pruebas.

5.3. Manejo de datos

Identifica directrices para la recopilación, el almacenamiento, la transmisión y la destrucción de datos de prueba, y establece requisitos detallados e inequívocos para el manejo de datos. Tenga en cuenta que los resultados de cualquier tipo de prueba de seguridad de la información identificarán vulnerabilidades que un adversario puede explotar y, por lo tanto, deben considerarse información confidencial.

6. Informes

Se detallan los requisitos de presentación de informes y los entregables que se esperan durante el proceso de pruebas y al finalizar este. Se debe incluir la información mínima que debe contener cada informe (por ejemplo, vulnerabilidades y técnicas de mitigación recomendadas) y la frecuencia de entrega (por ejemplo, informes de estado diarios). Se puede proporcionar una plantilla como anexo al documento de registro de evidencia (ROE) para ilustrar el formato y el contenido del informe.

7. Página de firmas

Diseñado para identificar a las partes responsables y garantizar que conozcan y comprendan sus responsabilidades durante todo el proceso de pruebas. Como mínimo, el líder del equipo de pruebas y la alta dirección de la organización (CSO, CISO, CIO, etc.) deben firmar el ROE (Registro de Evidencia) declarando que comprenden el alcance y los límites de la prueba.

Apéndice C—Pruebas y examen de seguridad de la aplicación

Las pruebas y el análisis de seguridad de aplicaciones ayudan a una organización a determinar si su software personalizado —por ejemplo, aplicaciones web— contiene vulnerabilidades explotables y si se comporta e interactúa de forma segura con sus usuarios, otras aplicaciones (como bases de datos) y su entorno de ejecución. La seguridad de las aplicaciones se puede evaluar de diversas maneras, desde la revisión del código fuente hasta las pruebas de penetración de la aplicación implementada.⁴³ Muchas pruebas de seguridad de aplicaciones someten la aplicación a patrones de ataque conocidos, típicos de su tipo. Estos patrones pueden atacar directamente la aplicación o intentar atacarla indirectamente, dirigiéndose al entorno de ejecución o a la infraestructura de seguridad. Algunos ejemplos de patrones de ataque son la fuga de información (por ejemplo, reconocimiento, exposición de información confidencial), la explotación de vulnerabilidades de autenticación y de gestión de sesiones, la subversión (por ejemplo, suplantación de identidad, inyección de comandos) y los ataques de denegación de servicio.

La evaluación de la seguridad de las aplicaciones debe integrarse en el ciclo de vida del desarrollo de software para garantizar su realización a lo largo de todo el ciclo. Por ejemplo, las revisiones de código pueden llevarse a cabo durante la implementación, en lugar de esperar a que la aplicación esté lista para las pruebas. También deben realizarse pruebas periódicamente una vez que la aplicación esté en producción; cuando se apliquen parches, actualizaciones u otras modificaciones importantes; o cuando se produzcan cambios significativos en el entorno de amenazas donde opera la aplicación.

Existen numerosas técnicas de análisis y pruebas de seguridad de aplicaciones. Estas se dividen en técnicas de caja blanca, que implican el análisis directo del código fuente de la aplicación, y técnicas de caja negra, que se realizan sobre el ejecutable binario de la aplicación sin conocer el código fuente.⁴⁴ La mayoría de las evaluaciones de aplicaciones personalizadas se realizan con técnicas de caja blanca, ya que el código fuente suele estar disponible; sin embargo, estas técnicas no detectan defectos de seguridad en las interfaces entre componentes, ni identifican problemas de seguridad causados durante la compilación, el enlazado o la configuración de la aplicación durante la instalación. Las técnicas de caja blanca tienden a ser más eficientes y rentables que las de caja negra para encontrar defectos de seguridad en aplicaciones personalizadas. Las técnicas de caja negra deben utilizarse principalmente para evaluar la seguridad de componentes compilados individuales de alto riesgo; las interacciones entre componentes; y las interacciones entre la aplicación o el sistema de aplicación completos con sus usuarios, otros sistemas y el entorno externo. También deben utilizarse para determinar la eficacia con la que una aplicación o sistema de aplicación gestiona las amenazas. Muchas pruebas combinan técnicas de caja blanca y de caja negra; esta combinación se conoce como pruebas de caja gris.

Los evaluadores que realizan evaluaciones de seguridad de aplicaciones deben poseer un conjunto básico de habilidades. Las directrices para el conjunto mínimo de habilidades incluyen el conocimiento de lenguajes y protocolos de programación específicos; el conocimiento del desarrollo de aplicaciones y las prácticas de codificación segura; la comprensión de las vulnerabilidades introducidas por malas prácticas de codificación; la capacidad de utilizar la revisión automatizada de código de software y otras herramientas de prueba de seguridad de aplicaciones; y el conocimiento de las vulnerabilidades comunes de las aplicaciones.

---

43 Algunos elementos de las pruebas de seguridad de aplicaciones, como las pruebas de penetración, son técnicas de validación de vulnerabilidades, no de identificación y análisis de objetivos. En esta sección, las pruebas de seguridad de aplicaciones se tratan únicamente por brevedad.

44 Algunas aplicaciones, como muchas aplicaciones web, no tienen ejecutables compilados (binarios), por lo que las técnicas de caja negra pueden no ser aplicables para analizar su código.

La seguridad de las aplicaciones cobra cada vez mayor importancia, ya que los atacantes se centran cada vez más en los ataques a la capa de aplicación. Debido a la complejidad de la evaluación de la seguridad de las aplicaciones, que abarca decenas de técnicas de uso común, esta publicación no pretende proporcionar información específica sobre dichas técnicas ni recomendaciones para su uso .⁴⁵ El Apéndice E incluye referencias con información adicional.

[45] En el futuro, el NIST podría publicar un documento aparte sobre pruebas y análisis de seguridad de aplicaciones.

Apéndice D—Pruebas de acceso remoto

Las pruebas de acceso remoto evalúan los métodos de acceso remoto en busca de vulnerabilidades y abarcan tecnologías como servidores de terminal, VPN, túneles Secure Shell (SSH), aplicaciones de escritorio remoto y módems de acceso telefónico.
Estas pruebas tienen como objetivo descubrir métodos alternativos de entrada a la red que eludan las defensas perimetrales. Las pruebas de acceso remoto suelen realizarse como parte de las pruebas de penetración, pero también pueden llevarse a cabo por separado para centrarse mejor en las implementaciones de acceso remoto. Las técnicas de prueba varían según el tipo de acceso remoto que se esté probando y los objetivos específicos de la prueba. Algunos ejemplos de técnicas comunes son:

Detección de servicios de acceso remoto no autorizados. El escaneo de puertos puede utilizarse para localizar puertos abiertos, que suelen estar asociados a servicios de acceso remoto. Los sistemas pueden revisarse manualmente en busca de servicios de acceso remoto mediante la visualización de los procesos en ejecución y las aplicaciones instaladas.

Revisar los conjuntos de reglas para detectar rutas de acceso remoto no deseadas. Los conjuntos de reglas de acceso remoto, como los de las puertas de enlace VPN, deben revisarse para detectar vulnerabilidades o configuraciones erróneas que podrían permitir accesos no autorizados.

Prueba de mecanismos de autenticación de acceso remoto. Dado que los métodos de acceso remoto normalmente requieren autenticación, los evaluadores deben verificar primero que se les exige autenticarse antes de intentar acceder. Pueden probar con cuentas y contraseñas predeterminadas (por ejemplo, cuentas de invitado o de mantenimiento) y realizar ataques de fuerza bruta. También pueden usar ingeniería social para intentar restablecer una contraseña o acceder sin un token de autenticación (por ejemplo, alegando que se ha perdido). Asimismo, pueden intentar acceder mediante programas de autenticación de autoservicio que permiten restablecer las contraseñas respondiendo a preguntas específicas del usuario.

Esto también puede implicar ingeniería social.

Supervisión de las comunicaciones de acceso remoto. Los evaluadores pueden supervisar las comunicaciones de acceso remoto mediante un analizador de red. Si las comunicaciones no están protegidas, los evaluadores podrían utilizarlas como fuente de información de autenticación de acceso remoto y otros datos enviados y recibidos por los usuarios de acceso remoto.

Las pruebas de acceso remoto activas o intrusivas deben realizarse en momentos de baja demanda para limitar las posibles interrupciones a los empleados y a los sistemas de acceso remoto.

Otro aspecto de las pruebas de acceso remoto es la evaluación de los sistemas telefónicos de una organización para detectar vulnerabilidades que permitan el acceso no autorizado o inseguro. La publicación NIST SP 800-24, Análisis de Vulnerabilidades de Centralitas Telefónicas (PBX)⁴⁶, proporciona información sobre los elementos y enfoques para las pruebas de seguridad de las centralitas telefónicas privadas (PBX). En el ámbito del acceso remoto, el principal objetivo de las pruebas de sistemas telefónicos son los módems; y aunque su uso ha disminuido debido a la amplia disponibilidad de acceso a redes cableadas e inalámbricas, se siguen produciendo ataques exitosos a través de módems no autorizados. Por ejemplo, hay usuarios que aún utilizan módems en sus ordenadores de trabajo para el acceso remoto, y algunas organizaciones utilizan tecnologías antiguas, como controladores y conmutadores de operaciones de edificios, que tienen módems de mantenimiento habilitados. Una sola vulneración a través de un módem podría permitir a un atacante el acceso directo e indetectado a una red, eludiendo la seguridad perimetral.

Varios programas informáticos permiten a los administradores de red (y a los atacantes) marcar grandes bloques de números de teléfono para buscar módems disponibles. Este proceso se denomina marcación masiva. Un ordenador con cuatro módems puede marcar 10 000 números en cuestión de días. Los programas de marcación masiva generan informes sobre los números con módems, y algunos incluso pueden intentar ataques automáticos limitados cuando se detecta un módem. Las organizaciones deberían realizar marcación masiva al menos una vez al año para identificar sus módems no autorizados.

---

46 Véase http://csrc.nist.gov/publications/PubsSPs.html Para obtener información adicional sobre la seguridad de la centralita telefónica (PBX).

Se realizan pruebas de módems fuera del horario laboral habitual para minimizar las posibles interrupciones a los empleados y al sistema telefónico de la organización. (Cabe mencionar, sin embargo, que muchos módems no autorizados pueden estar apagados fuera del horario laboral y pasar desapercibidos). También se puede utilizar la marcación automática para detectar equipos de fax. Las pruebas deben incluir todos los números de la organización, excepto aquellos que podrían verse afectados por un alto volumen de llamadas (por ejemplo, centros de operaciones 24 horas y números de emergencia).

Las habilidades necesarias para realizar pruebas de acceso remoto incluyen conocimientos de TCP/IP y redes; conocimientos de tecnologías y protocolos de acceso remoto; conocimientos de métodos de autenticación y control de acceso; conocimientos generales de sistemas de telecomunicaciones y funcionamiento de módems/PBX; y la capacidad de utilizar herramientas de escaneo y pruebas de seguridad como marcadores war.

[47] La mayoría de los programas de marcación de guerra permiten a los evaluadores excluir números específicos de la lista de llamadas.

Apéndice E—Recursos

Este apéndice incluye una amplia gama de recursos adicionales para su uso en pruebas y análisis de seguridad técnica. La tabla E-1 contiene una lista de documentos del NIST que complementan esta guía, y la tabla E-2 proporciona una lista de recursos en línea que las organizaciones pueden consultar para obtener información adicional.

Tabla E-1. Documentos NIST relacionados[48]

Documento del NIST	URL
SP 800-30, Guía de gestión de riesgos para sistemas de tecnología de la información	http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
SP 800-40 Versión 2.0, Creación de un programa de gestión de parches y	http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf
vulnerabilidades; SP 800-53 Revisión 2, Controles de seguridad recomendados para sistemas de información federales.	http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf
SP 800-53A, Guía para la evaluación de Controles de seguridad en la información federal Sistemas	http://csrc.nist.gov/publications/nistpubs/800-53A/SP800-53A-final-sz.pdf
SP 800-64 Revisión 1, Seguridad Consideraciones en la información Ciclo de vida del desarrollo de sistemas	http://csrc.nist.gov/publications/nistpubs/800-64/NIST-SP800-64.pdf
SP 800-84, Guía para pruebas, capacitación y Programas de ejercicios para planes de TI y Capacidades	http://csrc.nist.gov/publications/nistpubs/800-84/SP800-84.pdf
SP 800-92, Guía de seguridad informática Gestión de registros	http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf
SP 800-94, Guía de sistemas de detección y prevención de intrusiones (IDPS)	http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

Tabla E-2. Recursos en línea

Recurso	URL
Metodologías	
Equipo Rojo de Garantía de Diseño de Información (IDART)	http://www.idart.sandia.gov/
NIST SP 800-53A, Guía para la evaluación de la seguridad Controles en los sistemas de información federales	http://csrc.nist.gov/publications/PubsSPs.html
Información de la Agencia de Seguridad Nacional (NSA) Metodología de evaluación (IAM)	http://www.nsa.gov/ia/industry/education/iam.cfm?MenuID=10.2.4.2
Manual de metodología de pruebas de seguridad de código abierto (OSSTMM)	http://www.isecom.org/osstmm/
Proyecto de seguridad de aplicaciones web abiertas (OWASP) Proyecto de prueba	http://www.owasp.org/index.php/Category:OWASP_Testing_Project
Herramientas	
BackTrack (distribución en vivo para Linux)	http://www.remote-exploit.org/backtrack.html

[48] La URL base para todos los NIST SP es http://csrc.nist.gov/publications/PubsSPs.html

Recurso	URL
Extra – Knoppix (distribución en vivo para Linux)	http://www.knopper.net/knoppix-mirrors/index-en.html
FIRE (Distribución en vivo de Linux)	http://fire.dmzs.com/
Helix (distribución en vivo de Linux)	http://www.e-fense.com/helix/
INSERT Rescue Security Toolkit (distribución en vivo para Linux) http://www.inside-security.de/insert_en.html Distribución de herramientas	
de seguridad Knoppix (STD) (distribución en vivo de Linux) nUbuntu (distribución en	http://std.org/download.html
vivo de Linux)	http://www.nubuntu.org/downloads.php
Operador (distribución en vivo de Linux)	http://www.ussysadmin.com/operator/ http://
PHLAK (Distribución en vivo de Linux)	sourceforge.net/projects/phlakproject/
Las 100 mejores herramientas de seguridad de red	http://sectools.org/
Información sobre vulnerabilidades	
Enumeración de configuración común (CCE)	http://cce.mitre.org/ http://
Vulnerabilidades y exposiciones comunes (CVE)	cve.mitre.org/ http://
Enumeración de debilidades comunes (CWE)	cwe.mitre.org/ [Enlace
Lista de contraseñas predeterminadas	obsoleto eliminado]
Equipo francés de respuesta a incidentes de seguridad (FrSIRT)	http://www.frsirt.com/english/
Lista de avisos públicos de iDefense Lab	http://labs.idefense.com/intelligence/vulnerabilities/ http://
milw0rm	www.milw0rm.com/ http://
Base de Datos Nacional de Vulnerabilidad (NVD)	nvd.nist.gov/ http://
Archivos de Neohapsis	archives.neohapsis.com/
Base de datos de vulnerabilidades de código abierto	http://www.osvdb.org/
Proyecto de seguridad de aplicaciones web abiertas (OWASP) Vulnerabilidades	http://www.owasp.org/index.php/Category:Vulnerability
Avisos de Secunia	http://secunia.com/advisories/
Vulnerabilidades de SecurityFocus	http://www.securityfocus.com/vulnerabilidades
SecurityTracker	http://www.securitytracker.com/
Archivo de vulnerabilidades de Secwatch	http://secwatch.org/advisories/ http://
La elección del hacker (THC)	freeworld.thc.org/
Equipo de preparación para emergencias informáticas de Estados Unidos Base de datos de notas sobre vulnerabilidades (US-CERT)	http://www.kb.cert.org/vuls
Vulnerabilidades y Explotaciones Inalámbricas (WVE)	http://www.wirelessve.org/

Apéndice F—Glosario

A continuación se definen algunos términos utilizados en la publicación.

Pruebas de seguridad activas: Pruebas de seguridad que implican interacción directa con un objetivo, como el envío de paquetes a un objetivo.

Captura de banners: El proceso de obtener información de banners, como el tipo y la versión de la aplicación. que se transmite desde un puerto remoto cuando se inicia una conexión.

Pruebas encubiertas: Pruebas realizadas utilizando métodos encubiertos y sin el conocimiento del personal de TI de la organización, pero con el pleno conocimiento y permiso de la alta dirección.

Pruebas de seguridad externas: Pruebas de seguridad realizadas desde fuera del perímetro de seguridad de la organización.

Falso positivo: Una alerta que indica incorrectamente la presencia de una vulnerabilidad.

Comprobación de la integridad de los archivos: Software que genera, almacena y compara resúmenes de mensajes para archivos con el fin de detectar cambios realizados en los mismos.

Pruebas de seguridad de la información: El proceso de validar la implementación efectiva de los controles de seguridad para sistemas y redes de información, en función de los requisitos de seguridad de la organización.

Pruebas de seguridad internas: Pruebas de seguridad realizadas desde el interior del perímetro de seguridad de la organización.

Descubrimiento de red: El proceso de descubrir hosts activos y que responden en una red, identificar debilidades y aprender cómo funciona la red.

Análisis de red: Técnica pasiva que monitoriza la comunicación de red, decodifica protocolos y examina cabeceras y cargas útiles en busca de información de interés. Es tanto una técnica de revisión como de identificación y análisis de objetivos.

Identificación del sistema operativo (SO): Analizar las características de los paquetes enviados por un objetivo, como los encabezados de los paquetes o los puertos de escucha, para identificar el sistema operativo que se utiliza en el objetivo.

Pruebas abiertas: Pruebas de seguridad realizadas con el conocimiento y consentimiento del personal de TI de la organización.

Pruebas de seguridad pasivas: Pruebas de seguridad que no implican ninguna interacción directa con los objetivos, como el envío de paquetes a un objetivo.

Descifrado de contraseñas: El proceso de recuperar contraseñas secretas almacenadas en un sistema informático o transmitidas a través de una red.

Pruebas de penetración: Pruebas de seguridad en las que los evaluadores simulan ataques reales para identificar formas de eludir las medidas de seguridad de una aplicación, sistema o red. Estas pruebas suelen implicar la realización de ataques reales contra sistemas y datos reales, utilizando las mismas herramientas y técnicas que los atacantes. La mayoría de las pruebas de penetración buscan combinaciones de vulnerabilidades en uno o varios sistemas que permitan obtener un acceso mayor que el que se podría lograr con una sola vulnerabilidad.

Phishing: Una forma digital de ingeniería social que utiliza correos electrónicos de apariencia auténtica —pero falsos— para solicitar información a los usuarios o dirigirlos a un sitio web falso que solicita información.

Plan de Acción y Hitos (POA&M): Documento que identifica las tareas que deben realizarse. Detalla los recursos necesarios para llevar a cabo los elementos del plan, los hitos para el cumplimiento de las tareas y las fechas previstas de finalización de los hitos.

Escáner de puertos: Un programa que puede determinar de forma remota qué puertos de un sistema están abiertos (por ejemplo, si los sistemas permiten conexiones a través de esos puertos).

Técnicas de revisión: Técnicas de prueba de seguridad de la información pasivas, generalmente realizadas de forma manual, que se utilizan para evaluar sistemas, aplicaciones, redes, políticas y procedimientos para descubrir vulnerabilidades.
Incluyen la revisión de la documentación, los registros, los conjuntos de reglas y la configuración del sistema; el análisis de la red; y la comprobación de la integridad de los archivos.

Dispositivo no autorizado: Un nodo no autorizado en una red.

Reglas de Compromiso (RC): Directrices y restricciones detalladas para la ejecución de pruebas de seguridad de la información. Las RC se establecen antes del inicio de una prueba de seguridad y otorgan al equipo de pruebas la autoridad para realizar las actividades definidas sin necesidad de permisos adicionales.

Conjunto de reglas: Colección de reglas o firmas con las que se compara el tráfico de red o la actividad del sistema para determinar la acción a realizar, como reenviar o rechazar un paquete, crear una alerta o permitir un evento del sistema.

Ingeniería social: El proceso de intentar engañar a alguien para que revele información (por ejemplo, una contraseña).

Técnicas de identificación y análisis de objetivos: Técnicas de prueba de seguridad de la información, en su mayoría activas y generalmente realizadas con herramientas automatizadas, que se utilizan para identificar sistemas, puertos, servicios y posibles vulnerabilidades. Estas técnicas incluyen el descubrimiento de redes, la identificación de puertos y servicios de red, el escaneo de vulnerabilidades, el escaneo de redes inalámbricas y las pruebas de seguridad de aplicaciones.

Técnicas de validación de vulnerabilidades: Técnicas de prueba de seguridad de la información activas que corroboran la existencia de vulnerabilidades. Incluyen descifrado de contraseñas, pruebas de acceso remoto, pruebas de penetración, ingeniería social y pruebas de seguridad física.

Escaneo de versiones: Proceso de identificación de la aplicación de servicio y la versión de la aplicación que se está utilizando actualmente.

Máquina virtual (VM): Software que permite que un único host ejecute uno o más sistemas operativos invitados.

Vulnerabilidad: Debilidad en un sistema de información, o en los procedimientos de seguridad del sistema, los controles internos o la implementación, que podría ser explotada o activada por una fuente de amenaza.

Escaneo de vulnerabilidades: Técnica utilizada para identificar hosts/atributos de host y vulnerabilidades asociadas.

Apéndice G—Acrónimos y abreviaturas

A continuación se definen algunos acrónimos y abreviaturas utilizados en esta publicación.

ARP	Protocolo de resolución de direcciones
ATA	Accesorio de tecnología avanzada
CALIFORNIA	Certificación y acreditación
CCE	Enumeración de configuración común
CGE	Explotador global de Cisco
CIO	Director de Información
CIRT	Equipo de respuesta a incidentes informáticos
CISO	Director de Seguridad de la Información
director de tecnología	Director de Tecnología
CVE	Vulnerabilidades y exposiciones comunes
CVSS	Sistema común de puntuación de vulnerabilidades
CWE	Enumeración de debilidades comunes
DNS	Sistema de nombres de dominio
DoS	Denegación de servicio
DSL	Línea de abonado digital
FIPS	Normas federales de procesamiento de información
FISMA	Ley Federal de Gestión de la Seguridad de la Información
FrSIRT	Equipo francés de respuesta a incidentes de seguridad
FTP	Protocolo de transferencia de archivos
GOTS	Programas gubernamentales listos para usar
GPS	Sistema de Posicionamiento Global
Interfaz gráfica de usuario (GUI)	Interfaz gráfica de usuario
Departamento de Salud y Servicios Humanos	Departamento de Salud y Servicios Humanos
HTTP	Protocolo de transferencia de hipertexto
SOY	Metodología de evaluación de la información
ICMP	Protocolo de mensajes de control de Internet
IDART	Equipo Rojo de Garantía de Diseño de Información
IDPS	Sistema de detección y prevención de intrusiones
Sistema de detección de intrusiones (IDS)	Sistema de detección de intrusiones
IEEE	Instituto de Ingenieros Eléctricos y Electrónicos
IIS	Servidor de información de Internet
IP	Protocolo de Internet
IPS	Sistema de prevención de intrusiones
ISSO	Responsable de seguridad de sistemas de información
ÉL	Tecnologías de la información
ITL	Laboratorio de Tecnología de la Información
LAN	Red de área local
IMPERMEABLE	Control de acceso a los medios

NAT	Traducción de direcciones de red
NIS	Sistema de información de red
NIST	Instituto Nacional de Estándares y Tecnología
Agencia Nacional de Seguridad (NSA)	Agencia de Seguridad Nacional
NVD	Base de datos nacional de vulnerabilidad
OMB	Oficina de Administración y Presupuesto
sistema operativo	Sistema operativo
OSSTMM	Manual de metodología de pruebas de seguridad de código abierto
OWASP	Proyecto de seguridad de aplicaciones web abiertas
P2P	De igual a igual
Centralita telefónica	Intercambio de sucursales privadas
PDA	Asistente digital personal
Información personal identificable	Información de identificación personal
ALFILER	Número de identificación personal
POA&M	Plan de acción e hitos
ESTALLIDO	Protocolo de la oficina de correos
RF	Radiofrecuencia
HUEVA	Reglas de participación
SCADA	Control supervisorio y adquisición de datos
SCAP	Protocolo de automatización de contenido de seguridad
SHA	Algoritmo de hash seguro
SORBO	Protocolo de inicio de sesión
PYME	Experto en la materia
SMTP	Protocolo simple de transferencia de correo
SP	Publicación especial
SSH	Carcasa segura
SSID	Identificador de conjunto de servicios
SSL	Capa de conexiones seguras
Número de Seguro Social	Número de seguro social
ETS	Distribución de herramientas de seguridad
TCP	Protocolo de control de transmisión
TCP/IP	Protocolo de control de transmisión/Protocolo de Internet
TCP/UDP	Protocolo de control de transmisión/Protocolo de datagramas de usuario
TFTP	Protocolo trivial de transferencia de archivos
THC	La elección del hacker
UDP	Protocolo de datagramas de usuario
URL	Localizador uniforme de recursos
Certificación de EE. UU.	Equipo de preparación para emergencias informáticas de Estados Unidos
USB	Bus serie universal
Máquina virtual	Máquina virtual
VoIP	Protocolo de voz sobre Internet
VPN	Red privada virtual
PÁLIDO	Red de área amplia

WIDPS	Sistema inalámbrico de detección y prevención de intrusiones
WLAN	Red de área local inalámbrica
WVE	Vulnerabilidades y exploits inalámbricos
XML	Lenguaje de marcado extensible