Pruebas de penetración: Proteja los activos críticos con la mentalidad de un atacante

Identifique vulnerabilidades críticas utilizando las herramientas, técnicas y prácticas que utilizan los delincuentes

IBM Security

IBM

Tabla de contenido

2Resumen ejecutivo

2Desafíos de seguridad que se alinean con la necesidad de pruebas de penetración

3Qué proporciona la prueba de penetración

4Solución de IBM: IBM® X-Force® Red servicios de pruebas de penetración

4Pruebas de aplicaciones

5Pruebas de red

5Pruebas en humanos

6Pruebas de hardware

6Cajeros automáticos, Internet de las cosas (IoT) y pruebas específicas para automóviles

7El portal X-Force Red 7

Conclusión

Resumen ejecutivo

Defender a las empresas de los ciberdelincuentes se vuelve aún más importante a medida que aumenta la cantidad de datos valiosos y la regulación diseñada para protegerlos. De las 183 pruebas de penetración realizadas por IBM X-Force Red entre agosto de 2017 y noviembre de 2018, se identificaron 1099 vulnerabilidades, con un 12 % clasificado como alto o crítico.[1]Si los delincuentes pudieran explotar solo una vulnerabilidad de ese 12 por ciento, el impacto en una empresa podría ser perjudicial.

Los directores de información, los directores de seguridad de la información y otras personas a cargo de proteger sus negocios a menudo encuentran que identificar y corregir vulnerabilidades críticas es un desafío formidable. Las amenazas se dirigen a redes, hardware, aplicaciones, dispositivos y empleados desde dentro y fuera de sus organizaciones. A partir de sus compromisos de pruebas de penetración, X-Force Red determinó que las contraseñas débiles o predeterminadas y las credenciales codificadas representaban el 50 por ciento de las razones del compromiso del sistema. Entre octubre de 2017 y noviembre de 2018, el equipo envió 1176 correos electrónicos de phishing a organizaciones clientes; 198 personas hicieron clic en el enlace y 196 personas enviaron credenciales válidas.[2]

Con presupuestos, recursos y tiempo limitados para abordar tales amenazas, algunas organizaciones optan por utilizar herramientas automatizadas para probar sus entornos. Sin embargo, esas herramientas no están diseñadas para encontrar amenazas desconocidas, que a menudo son las que se escapan y tienen éxito.

Las pruebas de penetración manuales están diseñadas para ayudar a descubrir las vulnerabilidades conocidas y desconocidas más críticas en los entornos de las organizaciones. Las pruebas pueden ocurrir en cualquier cosa, desde redes, aplicaciones, hardware y otros sistemas hasta cajeros automáticos, automóviles, aviones, dispositivos IoT y más. Más organizaciones están reconociendo el valor de las pruebas manuales. Por ejemplo, el porcentaje de bancos que solicitaron X-Force Red para realizar pruebas en cajeros automáticos aumentó un 300 % de 2017 a 2018.[3]
Las pruebas de penetración pueden ayudar a las organizaciones a incorporar seguridad durante el diseño del producto y más allá, mantener el cumplimiento de los estándares normativos y proteger los datos confidenciales.

Desafíos de seguridad que se alinean con la necesidad de pruebas de penetración

Las debilidades de seguridad proliferan en las empresas por varias razones. Las empresas no siguen las mejores prácticas de seguridad y permiten a los empleados, contratistas y proveedores acceso ilimitado a todos sus activos. Este acceso ocurre sin importar el nivel de importancia de los activos ni el rol de las personas que acceden a ellos. Para complicar las cosas, más datos valiosos que nunca fluyen a través de redes, dispositivos, aplicaciones y personas, muchos de ellos en silos entre unidades de negocios. Esta infraestructura compleja dificulta la comprensión de las amenazas y vulnerabilidades dentro de sus activos más importantes.

Además, los tipos de amenazas van desde grupos criminales hasta estados nacionales y desde lobos solitarios hasta personas internas maliciosas y no maliciosas. Muchos delincuentes utilizan herramientas, técnicas y prácticas más sofisticadas que nunca, eludiendo sigilosamente los controles de seguridad y estafando al personal para que divulgue datos confidenciales.

Pruebas totales	Hallazgos totales	Crítico y de alto riesgo
183	1,099	136

*Figura 1.*De 183 pruebas realizadas desde agosto de 2017 hasta noviembre de 2018, X-Force Red encontró 1099 vulnerabilidades. De esas vulnerabilidades, 136 o 12 por ciento eran altas o críticas.[4]

Los requisitos reglamentarios también aumentan la presión y la complejidad en torno a la protección de datos. Por ejemplo, los requisitos de seguridad establecidos por el Estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS) se aplican a cualquier organización que maneje transacciones con tarjetas de pago. Independientemente del tamaño o la cantidad de transacciones, todas las empresas que entran en esta categoría deben completar algún nivel de cumplimiento con PCI DSS.

Otra regulación, el Reglamento General de Protección de Datos (GDPR), requiere que las organizaciones protejan los datos personales y la privacidad de los interesados europeos. No cumplir con el RGPD puede costarle a una organización hasta 20 millones de euros o el 4 por ciento de la facturación anual global, lo que sea mayor.

Las presiones comerciales diarias también crean vulnerabilidades. Los plazos ajustados para el cambio y la entrega al mercado de bienes y servicios pueden tener prioridad sobre la seguridad de los datos. Las fusiones y adquisiciones pueden hacer que una empresa herede más fallas en los datos durante la reorganización.

Teniendo en cuenta estos factores, una empresa que quiera ser proactiva en la protección de datos debería considerar incorporar pruebas de penetración.

Qué proporciona la prueba de penetración

Una prueba de penetración es una simulación de ataque y explotación diseñada para descubrir las debilidades de seguridad de un objetivo específico. Los piratas informáticos realizan estas pruebas con las herramientas, técnicas y prácticas que los delincuentes podrían usar para ingresar a un entorno y comprometer activos valiosos.

Las pruebas de penetración pueden ocurrir interna o externamente. El proceso evalúa el potencial para acceder a datos confidenciales y explotar las fallas del sistema. Las pruebas clasifican los hallazgos como críticos, altos, medios o bajos. Los resultados clasificados como críticos o altos son eventos probables que pueden comprometer un sistema más que amenazas teóricas.

Las organizaciones que realizan pruebas de penetración obtienen una comprensión de qué activos son vulnerables a un ataque y qué tipos de vulnerabilidades existen. Los probadores de penetración también muestran cómo un delincuente explotaría las vulnerabilidades. Los evaluadores pueden ayudar a las organizaciones a corregir esas debilidades antes de que los delincuentes las encuentren. El compromiso ofensivo ayuda a una organización a mantenerse por delante de los delincuentes.

Con las pruebas de penetración, los usuarios tienen la oportunidad de eludir las limitaciones del análisis de vulnerabilidades. El escaneo encontrará fallas conocidas, pero puede pasar por alto escenarios en los que los delincuentes pueden vincular múltiples vulnerabilidades para un ataque. Las técnicas que un delincuente conoce más allá de un centro de datos probablemente también escaparán a la detección del escaneo. El escaneo puede ser incompatible en algunos sistemas y componentes de hardware. Las pruebas manuales pueden ayudar a detectar vulnerabilidades que se pasan por alto en el análisis.

Realizar pruebas de penetración internamente tiene sus propias restricciones. La cantidad de pruebas necesarias para detectar vulnerabilidades críticas puede abrumar a un pequeño personal. Es probable que los equipos de seguridad no sepan acerca de las amenazas que atacan a otras empresas similares, ya que su único enfoque está en su organización específica. La rotación y la escasez de habilidades también pueden obstaculizar la efectividad de un equipo interno.

Los equipos externos de pruebas penetrantes pueden probar esencialmente cualquier cosa y todo. Combinan pruebas manuales y herramientas automatizadas para aumentar la eficacia en la búsqueda de vulnerabilidades conocidas y desconocidas. Pueden escalar más fácilmente ya que tienen equipos más grandes y más experiencia. Los equipos externos de pruebas de penetración también obtienen una visión más amplia del panorama de amenazas, ya que realizan pruebas para muchas organizaciones. Por lo general, estos grupos también tienen sus propios equipos de investigación y fuentes de inteligencia de amenazas.

Además, muchos equipos de prueba internos no tienen experiencia en automoción, dispositivos IoT y cajeros automáticos y los tratan de la misma manera que si trabajaran con computadoras. Estas verticales requieren experiencia, técnicas y herramientas de prueba específicas que los equipos de prueba de penetración externos pueden proporcionar.

Solución de IBM: servicios de pruebas de penetración de IBM X-Force Red

Los servicios de prueba de penetración X-Force Red de IBM Security ofrecen a los clientes las habilidades, la escala y el alcance para ayudarlos a encontrar y corregir las vulnerabilidades más peligrosas. El equipo de X-Force Red incluye cientos de piratas informáticos con décadas de experiencia en el acceso a organizaciones utilizando las mismas herramientas, técnicas, prácticas y mentalidad que los delincuentes. Los especialistas y desarrolladores experimentados entienden cómo crear código y dispositivos, y cómo los atacantes pueden comprometerlos. En un servicio ad hoc o de suscripción, los métodos de prueba que utiliza el equipo de X-Force Red incluyen pruebas manuales virtuales e in situ y escaneo automatizado.

Los clientes que utilizan los servicios de prueba de penetración de X-Force Red van desde marcas internacionales hasta operaciones más pequeñas en prácticamente todas las industrias. Independientemente del tamaño, el equipo de X-Force Red puede probar prácticamente cualquier red, aplicación, hardware, personal o dispositivo que desee una organización. El equipo puede realizar pruebas en los productos durante el desarrollo y después de que estén en el mercado. X-Force Red ha realizado pruebas de penetración para cientos de organizaciones y contando.

El equipo X-Force Red vende sus servicios utilizando un formato de "tarjeta de regalo". Como parte de sus servicios de suscripción, los clientes pagan una tarifa fija todos los meses y pueden cambiar lo que quieren probar en cualquier momento. La duración de las pruebas varía según el tamaño del entorno y las áreas probadas, como la cantidad de líneas de códigos.

Las consultas pueden ayudar a los clientes a determinar qué tipo de prueba es mejor para sus necesidades. Al final de la prueba, el equipo de X-Force Red presenta un informe de hallazgos, metodología utilizada y recomendaciones de remediación. Los clientes aprenden sobre las vulnerabilidades más graves que, si se explotan, podrían afectar más al negocio y lo que necesitan para remediar esas debilidades rápidamente.

El equipo de X-Force Red prueba aplicaciones, redes, humanos, hardware y más. El equipo también puede probar cajeros automáticos, automóviles y dispositivos integrados e IoT.

Pruebas de aplicaciones

Las aplicaciones son el corazón de muchas empresas. Si las aplicaciones críticas fallan, el negocio también se detiene.

Para proteger sus aplicaciones, algunas organizaciones confían en controles de seguridad automatizados. Sin embargo, esos controles solo pueden abordar ataques automatizados. Solo los humanos pueden detectar y abordar ataques manuales basados en humanos.

Otras organizaciones utilizan firewalls de aplicaciones; sin embargo, estos fallan en la lógica (qué está haciendo la aplicación y por qué) que los delincuentes a menudo eluden y explotan. Además, las aplicaciones pueden tener malware, que puede infectar los sistemas de las organizaciones cuando se instala.

El equipo de X-Force Red realizó 24 pruebas de aplicación para organizaciones entre agosto y noviembre de 2018. Los hallazgos incluyen lo siguiente:

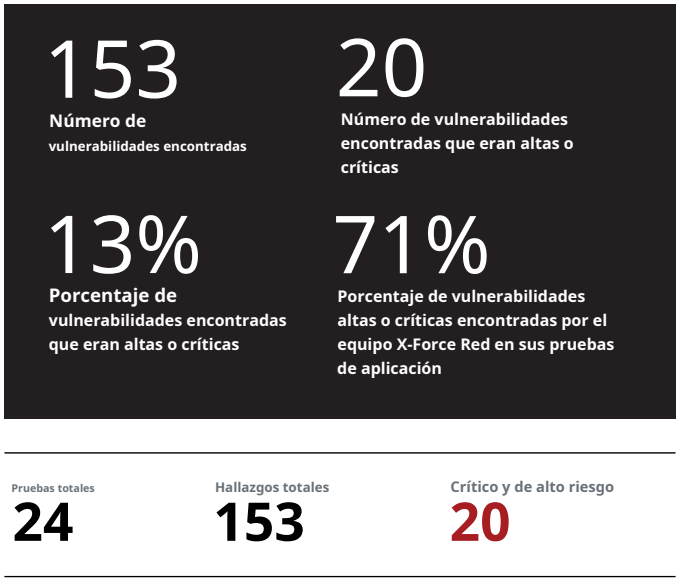

*Figura 2.*Para las pruebas de aplicaciones, 24 pruebas realizadas desde agosto hasta noviembre de 2018 encontraron 153 vulnerabilidades. De esas vulnerabilidades, 20 pruebas o el 13 por ciento fueron altas o críticas.

Para mitigar estas fallas, el equipo de X-Force Red prueba manualmente las aplicaciones para identificar vulnerabilidades en los procesos y controles de seguridad que los desarrolladores pueden haber pasado por alto. Los evaluadores validan las vulnerabilidades conocidas y "todavía desconocidas" y eliminan los falsos positivos.

El equipo de X-Force Red también puede realizar una revisión del código fuente de la aplicación. Los clientes pueden proporcionar su código fuente para permitir pruebas más rentables y en tiempo.

Más juntas directivas requieren pruebas de seguridad de aplicaciones, ya que las aplicaciones críticas son las que mantienen el negocio en funcionamiento. Al mismo tiempo, más mandatos de cumplimiento de la industria comienzan a requerir pruebas de penetración, como PCI DSS. Las pruebas de aplicaciones de X-Force Red ayudan a los clientes a abordar los mandatos de cumplimiento e incorporar seguridad antes y después de que las aplicaciones se lancen al mercado.

Pruebas de red

El uso de tecnologías de proveedores externos podría poner en riesgo las redes de la empresa. Los proveedores pueden no seguir las políticas y los procedimientos de seguridad. Y las empresas pueden instalar estas tecnologías sin seguir las mejores prácticas de seguridad.

Además, algunas empresas pueden carecer de cifrado en las comunicaciones internas u otras aplicaciones en la red. Con estas deficiencias, los delincuentes pueden descifrar contraseñas y acceder a los servidores de las empresas, máquinas virtuales, datos de clientes, copias de seguridad de bases de datos y más.

El equipo de X-Force Red puede ayudar a identificar estos problemas mediante pruebas de penetración de red manuales. La evaluación mide la seguridad de los dispositivos desde una perspectiva de red, centrándose en los servicios expuestos, las configuraciones y la infraestructura. La prueba identifica ataques oportunistas que los delincuentes pueden ejecutar y vulnerabilidades que los escáneres podrían no detectar.

Usando las mismas herramientas, técnicas, prácticas y mentalidad que los delincuentes, los evaluadores de X-Force Red ingresan a la infraestructura de red de las organizaciones para identificar vulnerabilidades. El equipo identifica fallas, como si los hosts de la red tienen una relación de confianza activa con otro host que es susceptible a un ataque. Las pruebas generalmente se realizan durante el horario comercial cuando los empleados usan la red y pueden responder de inmediato cuando se necesita una solución rápida. Los proyectos suelen tardar de una a dos semanas, según el tamaño de la red.

Con las pruebas de red, los clientes aprenden a realizar cambios programáticos diseñados para ayudar a fortalecer la protección en sus redes y en toda su infraestructura. Las pruebas de red también ayudan a los líderes de seguridad a comprender dónde invertir sus recursos para minimizar al máximo el riesgo.

Pruebas de personal

Si bien más empresas están realizando capacitaciones de concientización sobre seguridad, algunas aún no educan a sus empleados en absoluto o con la frecuencia suficiente. Incluso los mejores controles de seguridad no pueden evitar algunos ataques dirigidos a los empleados.

Como se mencionó anteriormente, X-Force Red descubrió que las contraseñas débiles o predeterminadas y las credenciales codificadas fueron las principales razones para un compromiso. Otro desafío es combatir el phishing, donde los delincuentes envían correos electrónicos persuadiendo a los empleados para que revelen información personal.

El equipo de X-Force Red utiliza técnicas de ingeniería social para crear artimañas similares a las empleadas por los delincuentes. Los evaluadores analizan qué personal interactuó con correos electrónicos maliciosos. También realizan ejercicios de vishing o phishing de voz para ver qué información confidencial divulgan los empleados por teléfono a una persona no verificada.

Otras pruebas pueden incluir cargar unidades USB con contenido falso y engañar a los usuarios para que conecten el dispositivo. Para las pruebas de seguridad física, el equipo de X-Force Red evalúa las políticas y los procedimientos al intentar acceder a áreas seguras e información confidencial en la propiedad de la empresa. Algo tan simple como una caja de donas puede hacer que los hackers de X-Force Red entren en la puerta.

Cuando finaliza la prueba, el equipo de X-Force Red proporciona una lista priorizada de recomendaciones personalizadas para ayudar a mitigar las vulnerabilidades identificadas.

Pruebas de hardware

Los delincuentes que quieren comprometer un dispositivo a menudo tienen pocos obstáculos. Pueden comprar el mismo modelo, romper el interior, encontrar sus vulnerabilidades y usar ese conocimiento para explotar fallas que exponen a su objetivo. Muchos dispositivos de hardware carecen de cifrado para los datos almacenados y tienen información de funcionalidad en el dispositivo durante la producción. Los delincuentes pueden encontrar un modelo de dispositivo, recuperar las credenciales predeterminadas y comprometer el dispositivo de un objetivo utilizando las mismas credenciales.

Los probadores de X-Force Red revisan cómo se construyen los productos de principio a fin. La prueba tiene como objetivo todo lo electrónico y el recinto o carcasa que forma parte del dispositivo. Los probadores de X-Force Red también ayudan a seleccionar e implementar piezas y controles para que la seguridad esté integrada en el producto en lugar de ser una ocurrencia tardía.

El equipo X-Force Red ofrece dos tipos de pruebas de hardware. Para las pruebas de "caja blanca", los clientes proporcionan documentación de diseño, código fuente y esquemas de diseño. El equipo de X-Force Red revisa el código fuente y los datos que entran y salen del sistema e identifica vulnerabilidades en la implementación del producto y bibliotecas externas. Para las pruebas de "caja negra", el equipo de X-Force Red aplica ingeniería inversa a los productos para recrear la documentación de diseño. Este proceso prueba las vulnerabilidades dentro del ciclo de vida de un producto, incluido el código fuente y la implementación.

Cajeros automáticos, IoT y pruebas específicas para automóviles

El equipo de X-Force Red tiene décadas de experiencia probando cajeros automáticos, automóviles, IoT, puntos de venta y otros dispositivos. Los evaluadores se enfocan en investigar, probar y brindar orientación para asegurar estos sistemas durante el diseño y más allá. El equipo de X-Force Red tiene una visión global de las fallas y vulnerabilidades de estos sistemas y puede brindar asistencia práctica cuando sea necesario.

Considere los cajeros automáticos. Su omnipresencia en lugares dispares con miles de dólares en efectivo físico atrae a los delincuentes.

Desde enero hasta octubre de 2018, el equipo de X-Force Red descubrió que los principales problemas de seguridad de los cajeros automáticos eran la falta de cifrado de disco completo y los candados deficientes en los gabinetes. Un probador rompió la cerradura de un gabinete de cajero automático en 20 segundos.

Los bancos reconocen la gravedad de estas amenazas como lo muestra la siguiente figura:

300%

Porcentaje de aumento de los bancos que solicitan al equipo X-Force Red para realizar pruebas de cajeros automáticos 2017-2018. Solo en Asia Pacífico, hubo un aumento de cinco veces en las solicitudes de pruebas de cajeros automáticos.

El aumento se debe en parte a una advertencia del FBI sobre la proliferación de ataques de "retiro de efectivo" en cajeros automáticos. La siguiente figura ilustra esta amenaza:

Advertencia del FBI: ataques de retiro de efectivo

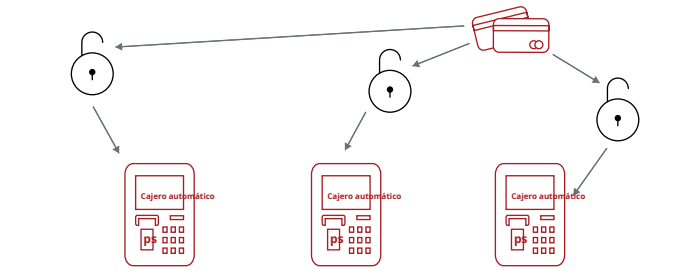

*Figura 3.*En los ataques de "retiro de efectivo", los delincuentes manipulan los límites de retiro y crean tarjetas de cajero automático fraudulentas para sacar efectivo, lo que podría agotar la cuenta completa del cliente.

El equipo de X-Force Red ofrece a los clientes pruebas en cajeros automáticos in situ, pruebas virtuales y otra opción. Los clientes pueden enviar cajeros automáticos e IoT, dispositivos específicos para automóviles y dispositivos electrónicos similares a X-Force Red Labs para realizar pruebas.

X-Force Red tiene cuatro laboratorios ubicados en Austin, Texas y Atlanta, Georgia en los Estados Unidos, Hursley en el Reino Unido y Melbourne, Australia. Dentro de los laboratorios, los evaluadores separan dispositivos de hardware específicos para identificar debilidades. Evalúan la composición del hardware, la interacción con el software y asuntos relacionados. Los probadores de X-Force Red también establecen objetivos de productos, crean requisitos de seguridad y modelan amenazas para descubrir vulnerabilidades. Pueden ayudar a las empresas a corregir fallas de seguridad antes de que los productos salgan al mercado para evitar posibles pérdidas financieras y daños a la marca.

El portal X-Force Red

Para todos los clientes, el portal X-Force Red proporciona comunicación y colaboración convenientes, directas y protegidas con los probadores. Usando el portal, que es una plataforma basada en la nube, los clientes pueden solicitar pruebas en un formulario encriptado. Los clientes pueden contactar a los evaluadores directamente desde el portal con cualquier pregunta o comentario en cualquier momento, evitando el intercambio de correos electrónicos y llamadas telefónicas.

El portal X-Force Red permite una reparación más rápida en tiempo real. Tradicionalmente, los evaluadores escriben sus informes una o dos semanas después de concluir el proyecto. Este tiempo de retraso significa que los clientes deben esperar los hallazgos, lo que les da a los delincuentes más tiempo para atacar, mientras pueden aparecer nuevas vulnerabilidades. Usando el portal X-Force Red, los evaluadores envían sus hallazgos cuando los identifican, lo que ofrece al cliente la oportunidad de ver y remediar las vulnerabilidades rápidamente. Al proporcionar una vista del progreso y los resultados de las pruebas, el portal ayuda a los clientes y evaluadores a mantenerse informados sobre la situación.

Los informes interactivos ingresados en el portal contienen hallazgos clave sobre vulnerabilidades, evidencia de explotación y orientación detallada para priorización y remediación. Al ingresar informes en el portal, X-Force Red permite a los líderes de seguridad determinar quién tiene permiso para ver los resultados. Los clientes pueden aislar secciones del informe en segmentos para que las personas solo vean las vulnerabilidades dentro de su alcance. A lo largo del proceso, los líderes de seguridad mantienen el control de la determinación de soluciones para sus organizaciones.

El portal X-Force Red actúa como depósito central de todos los informes para los clientes. Las organizaciones que realizan múltiples pruebas pueden monitorear, rastrear y revisar todos los informes en tiempo real. Los clientes reciben un registro histórico para comparar las fallas encontradas y las mejoras realizadas a lo largo del tiempo.

El portal también tiene sus propios controles de seguridad, que incluyen Secure Sockets Layer (SSL), encriptación, autenticación de dos factores y más.

Conclusión

La proliferación de demandas judiciales potenciales, pérdidas financieras y daños a la marca derivados de violaciones de seguridad significa que las organizaciones deben ser proactivas en la protección de sus activos más valiosos. Con los servicios de pruebas de penetración de IBM X-Force Red, los clientes pueden identificar y corregir vulnerabilidades críticas antes de que los delincuentes las exploten. Los evaluadores de X-Force Red tienen décadas de experiencia en la identificación y explotación de fallas utilizando las mismas herramientas, técnicas y prácticas que los delincuentes. Debido a su mentalidad de atacante, los evaluadores de X-Force Red también encuentran nuevas formas de comprometer organizaciones que los delincuentes pueden no haber probado. Como resultado, las organizaciones que utilizan los servicios de pruebas de penetración de X-Force Red para encontrar y corregir fallas críticas en sus infraestructuras pueden desarrollar controles que las ayuden a fortalecer sus medidas de seguridad para adelantarse a los delincuentes.

Para más información

Para obtener más información sobre las pruebas de penetración, comuníquese con su representante de IBM o IBM Business Partner, o visite **ibm.com/seguridad.**

Corporación IBM
Nuevo camino de la huerta
Armonk, Nueva York 10504

Producido en los Estados Unidos de
América Enero 2019

1. Hallazgos de las pruebas de penetración de X-Force Red, agosto de 2017 a noviembre de 2018.
2. Hallazgos de las pruebas de penetración de X-Force Red, octubre de 2017 a noviembre de 2018.
3. Presentación de prueba de cajero automático X-Force Red, noviembre de 2018.
4. Resultados de las pruebas de penetración de X-Force Red, agosto de 2017 a noviembre de 2018.

17023217USEN-00