Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1214

(03/2018)

SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

Seguridad en el ciberespacio – Ciberseguridad

Técnicas de evaluación de la seguridad en las redes de telecomunicaciones/tecnologías de la información y la comunicación

Recomendación UIT-T X.1214

UIT-T

Unión Internacional de Telecomunicaciones

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD (1)	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web	X.1140–X.1149
Protocolos de seguridad (1)	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	**X.1200–X.1229**
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD (2)	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1319
Seguridad de las redes eléctricas inteligentes	X.1330–X.1339
Correo certificado	X.1340–X.1349
Seguridad de la Internet de las cosas (IoT)	X.1360–X.1369
Seguridad en los sistema de transporte inteligente (ITS)	X.1370–X.1389
Seguridad de tecnología de libro mayor distribuido	X.1400–X.1429
Protocolos de seguridad (2)	X.1450–X.1459
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Aspectos generales de la ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/heurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de heurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	
Visión general de la seguridad de la computación en nube	X.1600–X.1601
Diseño de la seguridad de la computación en nube	X.1602–X.1639
Prácticas óptimas y directrices en materia de seguridad de la computación en nube	X.1640–X.1659
Aplicación práctica de la seguridad de la computación en nube	X.1660–X.1679
Otras cuestiones de seguridad de la computación en nube	X.1680–X.1699

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T X.1214

Técnicas de evaluación de la seguridad en las redes de telecomunicaciones/tecnologías de la información y la comunicación

Resumen

En la Recomendación UIT-T X.1214 se describe una metodología de evaluación de la seguridad de los elementos de redes de telecomunicaciones/tecnologías de la información y la comunicación (TIC) basados en soporte lógico y prácticas idóneas para promotores, fabricantes, operadores y expertos en seguridad en el campo de las telecomunicaciones para abordar la cuestión de la seguridad de sus elementos basados en soporte lógico. Las redes tradicionales de conmutación de circuitos y las redes basadas en paquetes están expuestas a diferentes amenazas y ataques –tanto de fuentes externas como internas– dirigidas a diversas partes de las redes de telecomunicaciones/TIC. En lo relativo a las redes de telecomunicaciones/TIC, la presente Recomendación aborda:

– detección de vulnerabilidades;

– metodología de evaluación de la seguridad.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1214	2018-03-29	17	11.1002/1000/13404

Palabras clave

Análisis binario, fuzzing, prueba de penetración, evaluación de la seguridad, prueba de seguridad, examen del código fuente, búsqueda de vulnerabilidades.

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Introducción

Las redes de telecomunicaciones/TIC desempeñan en el crecimiento económico de la mayoría de los países un papel fundamental. Esto ha llevado a que los gobiernos reglamenten la industria de las telecomunicaciones, incluso imponiendo requisitos para garantizar la seguridad de los equipos y redes de telecomunicaciones. Los operadores de telecomunicaciones deben adoptar programas de seguridad robustos y gestionados para asegurarse de que sus elementos basados en soporte lógico de sus redes están protegidos contra ataques malignos, tanto internos como externos, garantizando al mismo tiempo la adaptación al entorno reglamentario local. Para ello se necesitan mecanismos de evaluación de la seguridad muy eficaces, para esos elementos basados en soporte lógico, basados en normas y prácticas idóneas en materia de seguridad aceptadas a nivel mundial.

Conservar una posición de seguridad coherente en toda la red de una organización frente a la naturaleza cambiante de las amenazas es una tarea compleja y que lleva mucho tiempo. Es posible que las organizaciones tengan que incurrir en fuertes gastos para remediar una brecha de seguridad. Esos gastos responderán a las actividades de remedio, a programas de protección y conservación del consumidor, actividades de orden jurídico, la pérdida de socios comerciales, una mejor productividad por empleado y una reducción de los ingresos. Una evaluación de la seguridad eficaz evitará esas hemorragias financieras al identificar proactivamente los riesgos en sus activos y capacidades basados en soporte lógico y eliminarlos antes de que se produzcan los ataques o se abran las brechas de seguridad. En sectores como el estatal, el financiero y el de telecomunicaciones hay una creciente demanda de evaluaciones de seguridad independientes.

En esta Recomendación se ponen de manifiesto las técnicas de evaluación de la seguridad que deberán adoptar los operadores de redes de telecomunicaciones/TIC y los proveedores de servicio para identificar y evaluar las vulnerabilidades en sus elementos basados en soporte lógico.

Recomendación UIT-T X.1214

Técnicas de evaluación de la seguridad en las redes de telecomunicaciones/tecnologías de la información y la comunicación

1 Alcance

En esta Recomendación se abordan las técnicas de evaluación de la seguridad que pueden utilizarse en elementos basados en soporte lógico de las redes de telecomunicaciones/tecnologías de la información y la comunicación (TIC). Las redes tradicionales de conmutación de circuitos y las redes basadas en paquetes están expuestas a diferentes amenazas y ataques -tanto de fuentes externas como internas- dirigidas a diversas partes de los elementos basados en soporte lógico de una red de telecomunicaciones/TIC. Evaluar la seguridad de los componentes basados en soporte lógico antes de su despliegue en las redes puede ayudar a los operadores y proveedores de servicio a aumentar en gran medida la fiabilidad de las redes. Es, por tanto, necesario realizar un ejercicio de normalización en esta esfera a fin de que los creadores, fabricantes, operadores y expertos en seguridad puedan disponer de normas y prácticas idóneas en materia de evaluación de la seguridad de elementos basados en soporte lógico aceptadas a nivel mundial.

Estas técnicas pueden utilizarse individualmente o combinadas, según se prefiera o sea adecuado.

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

[UIT-T X.1520] Recomendación UIT-T X.1520 (2014), *Vulnerabilidades y exposiciones comunes*

[UIT-T X.1524] Recomendación UIT-T X.1524 (2012), *Lista de puntos débiles comunes*

[UIT-T X.1544] Recomendación UIT-T X.1544 (2013), *Enumeración y clasificación de pautas de ataques comunes*

3 Definiciones

3.1 Términos definidos en otros documentos

Esta Recomendación utiliza los siguientes términos definidos en otros documentos:

3.1.1 repositorio [UIT-T X.1524]: Conjunto implícito o explícito de datos sobre puntos débiles del soporte lógico relacionados con la seguridad que soporta una herramienta dada, por ejemplo, una base de datos sobre puntos débiles, el conjunto de patrones de un analizador de código o un sitio web.

3.1.2 vulnerabilidad [UIT-T X.1520]: Un punto débil en el software que podría ser utilizada para violar un sistema o la información que contiene.

3.1.3 punto débil [UIT-T X.1524]: Error o imperfección presente en el código, el diseño, la arquitectura o la ejecución del software que puede, en un momento dado, convertirse en una vulnerabilidad o favorecer la aparición de otras vulnerabilidades.

3.2 Términos definidos en esta Recomendación

En la presente Recomendación se definen los siguientes términos:

3.2.1 análisis binario: Técnica de identificación de puntos débiles en ficheros ejecutables en leguaje de máquinas.

3.2.2 *fuzzing*: Técnica destinada a descubrir vulnerabilidades desconocidas o del día cero introduciendo datos inesperados y buscando excepciones en las respuestas.

3.2.3 mutación: Modificación de bytes, palabras o cadenas mediante la introducción de un paquete de datos.

3.2.4 prueba de penetración: Técnica para evaluar las consecuencias de la explotación de las vulnerabilidades identificadas.

3.2.5 evaluación de seguridad: Estudio explícito para detectar vulnerabilidades y riesgos de seguridad.

3.2.6 exploración por firma: Técnica de exploración que compara los contenidos del objetivo con la base de datos de firmas conocidas para identificar vulnerabilidades.

Si una firma concreta coincide, el explorador identifica la vulnerabilidad y sugiere medidas correctivas.

3.2.7 examen del código fuente: Técnica de identificación de puntos débiles en segmentos del código fuente escritos en lenguajes de alto nivel.

3.2.8 herramienta: Aplicación de software o dispositivo que examina un anfitrión, una red, una parte de un software, un binario, una aplicación de software, un dispositivo o cualquier otro artefacto y facilita información sobre sus vulnerabilidades, puntos débiles o riesgos, por ejemplo, un explorador de vulnerabilidades, un *fuzzer*, una herramienta de examen de código fuente, un analizador binario, una herramienta de prueba de penetración, etc.

3.2.9 exploración de vulnerabilidades: Técnica de identificación de las vulnerabilidades conocidas o registradas en un objetivo.

4 Abreviaturas y acrónimos

Esta Recomendación hace uso de las siguientes abreviaturas y acrónimos:

CAPEC Enumeración y clasificación de pautas de ataques comunes *(Common Attack Pattern Enumeration and Classification)*

CVE Vulnerabilidades y exposiciones comunes *(Common Vulnerabilities and Exposures)*

CWE Enumeración común de debilidades *(Common Weakness Enumeration)*

DUT Dispositivo que se prueba (*Device Under Test)*

OS Sistema operativo *(Operating System)*

SQL Lenguaje de consulta estructurado (*Structured Query Language)*

TIC Tecnologías de la información y la comunicación

5 Convenios

Ninguno.

6 Concepto básico – prueba de seguridad

Las redes de telecomunicaciones/TIC tienen probabilidades de ser una mezcla heterogénea de equipos de distintos proveedores. Es necesario contar con un programa de certificación por terceros

fiable y con gran credibilidad para realizar un examen que identifique y evalúe los puntos débiles y vulnerabilidades de seguridad del software, el firmware y el hardware de los equipos. La evaluación de la seguridad de un producto se centra principalmente en la detección y la validación de las vulnerabilidades que presenta. La detección de vulnerabilidades puede dividirse en dos grandes categorías (véanse las cláusulas 6.1 y 6.2).

6.1 Detección de vulnerabilidades conocidas o registradas

Los productos de software de uso cotidiano suelen presentar vulnerabilidades. Estas vulnerabilidades, por ejemplo las vulnerabilidades y exposiciones comunes (CVE), se registran en la *National Vulnerability Database* y en otras bases de datos. Una gestión eficiente de las vulnerabilidades registradas es, por tanto, una actividad importante en los esfuerzos por la seguridad de las empresas modernas. Hacer un seguimiento manual de todas las vulnerabilidades presentes en los sistemas y ponerles solución adecuadamente es una tarea que necesita esfuerzos ingentes. Existen herramientas automatizadas que efectúan exploraciones por firmas para detectar esas vulnerabilidades e identificarlas según [b-CVE].

6.2 Detección de vulnerabilidades desconocidas o del día cero

Este tipo de detección consiste en descubrir vulnerabilidades que hasta la fecha no se han registrado. Para ello existen varios métodos que ofrecen diversas ventajas y desventajas. No hay ningún método completo y ninguno de ellos puede por sí solo descubrir todas las vulnerabilidades posibles del objetivo en cuestión. Entre las herramientas y técnicas utilizadas para detectar vulnerabilidades desconocidas o del día cero se cuentan los *fuzzers*, las herramientas de examen del código fuente y las herramientas de análisis binario, cuyos detalles se tratan en las cláusulas 7.2 a 7.5.

7 Técnicas de pruebas de seguridad

Como ya se ha indicado, existen distintos métodos para detectar vulnerabilidades en los elementos basados en soporte lógico y cada uno de ellos tiene sus propias ventajas e inconvenientes. No hay un solo método que pueda descubrir todas las vulnerabilidades posibles del objetivo en cuestión, por lo que un mecanismo de evaluación efectivo con toda probabilidad combinará los múltiples métodos que se tratan en las cláusulas 7.1 a 7.5.

7.1 Exploración de vulnerabilidades

El explorador de vulnerabilidades de red es un dispositivo o software que se utiliza para explorar la arquitectura de la red y dar cuenta de todas las vulnerabilidades identificadas en elementos basados en soporte lógico de la red. Mientras se realiza la exploración, se compara una base de datos de firmas de vulnerabilidades con la información obtenida de la exploración de la red a fin de crear una lista de las vulnerabilidades que con probabilidad existen en la red. En ocasiones el explorador comprende también una herramienta de prueba de penetración a fin de poder explotar realmente las vulnerabilidades identificadas y verificar fehacientemente su presencia. El análisis de vulnerabilidades es el proceso de evaluación de la gravedad de las vulnerabilidades identificadas. Las organizaciones suelen tener un gran número de vulnerabilidades en su entorno operativo y algunas de ellas pueden plantear un riesgo para la seguridad más elevado que otras. Por ejemplo, algunas vulnerabilidades de software tendrían consecuencias funestas si llegaran a explotarse. Es, por consiguiente, importante evaluar los problemas más importantes y ponerles remedio en primer lugar.

La exploración de vulnerabilidades puede realizarse en sistemas conectados a Internet y en redes internas que no están conectadas a Internet a fin de evaluar las vulnerabilidades del software.

De acuerdo con los requisitos y funcionalidades especificados en [UIT-T X.1520], las herramientas, repositorios y servicios utilizados para la exploración de vulnerabilidades deben ser compatibles con CVE.

7.2 *Fuzzing*

Por *fuzzing* se entiende el método de descubrimiento de vulnerabilidades desconocidas o del día cero en software mediante la introducción de datos inesperados y la búsqueda de excepciones en las respuestas. Suele ser un proceso total o parcialmente automatizado que implica la manipulación e introducción repetida de datos en el software objetivo para su procesamiento. El software objetivo puede ser una pila de protocolo, una aplicación o un fichero, en función de lo cual se utilizará el *fuzzer* adaptado. Los investigadores o probadores no necesitan conocer el funcionamiento interno del objetivo y por ese motivo este método se denomina también prueba de la caja negra.

Hay dos grandes tipos de *fuzzing*, a saber, el *fuzzing* por generación y el *fuzzing* por mutación, que se describen en las cláusulas 7.2.1 y 7.2.2, respectivamente.

7.2.1 *Fuzzing* por generación

Cuando se utiliza este método, se empieza por estudiar una especificación concreta para entender todas las estructuras de datos soportadas y las gamas de valores aceptables de cada una de ellas. A continuación se generan los datos que se van a introducir en el objetivo para probar las condiciones de frontera o violar directamente la especificación. La creación de las pruebas puede necesitar una cantidad considerable de trabajo previo, pero ofrece la ventaja de poder reutilizarlas para probar múltiples implementaciones del mismo protocolo o formato de fichero.

7.2.2 *Fuzzing* por mutación

Los *fuzzers* por mutación inducen la mutación de las muestras de datos existentes con paquetes relacionados con el objetivo para crear las pruebas. Cada byte, palabra o cadena de esas muestras se modifica y envía al objetivo. Este método necesita muy poco estudio previo y puede prepararse en muy poco tiempo. Sin embargo, no se trata de un método muy eficaz, pues puede necesitar de la obtención de numerosas muestras de datos para cubrir convenientemente el protocolo objetivo.

Los *fuzzers* son muy eficaces para los problemas que pueden causar que un programa colapse, como el desbordamiento de la memoria intermedia, la ejecución de scripts en otros sitios (*cross-site scripting*), los ataques de denegación de servicio, los errores de formato y la inyección de lenguaje de consulta estructurado (SQL). El *fuzzing* es menos eficaz para las amenazas de seguridad que no provocan el colapso de los programas, como los software espía (*spyware*), algunos virus, gusanos, caballos de Troya o registros de contraseñas.

De acuerdo con los requisitos y funcionalidades especificados en [UIT-T X.1524], las herramientas, repositorios y servicios utilizados para el *fuzzing* deben ser compatibles con la enumeración común de vulnerabilidades (CWE).

7.3 Examen del código fuente

El examen del código fuente es un método que los creadores de software utilizan comúnmente para encontrar los puntos débiles o fallos y también se conoce como prueba de la caja blanca. Puede llevarse a cabo manualmente o con asistencia de herramientas automatizadas. Dado que los programas de software suelen estar formados por millones de líneas de código, el examen meramente manual suele ser imposible. Las herramientas automatizadas son un valiosísimo recurso que facilita la tarea, pero sólo puede identificar los segmentos de código sospechosos o potencialmente vulnerables. En ocasiones es necesario llevar a cabo un análisis manual para determinar si los problemas detectados lo son realmente, pues esta herramienta también arroja resultados falsamente positivos. La mayor limitación de este método reside en que los vendedores o fabricantes son reacios a compartir su código fuente.

De acuerdo con los requisitos y funcionalidades especificados en [UIT-T X.1524], las herramientas, repositorios y servicios utilizados para el examen de código fuente deben ser compatibles con la enumeración común de vulnerabilidades (CWE).

7.4 Análisis binario

La evaluación de la seguridad empleando instrucciones en lenguaje de máquina, en lugar de código fuente, suele denominarse análisis binario. Con este análisis se crea un modelo de comportamental analizando el flujo de control y datos de una aplicación mediante código de máquina ejecutable, que es como lo ven los agresores. A diferencia de lo que ocurre con las herramientas de código fuente, con este método se detectan precisamente los problemas en la aplicación núcleo y también las vulnerabilidades en las bibliotecas de terceros, en los componentes preinsertados y el en código introducido por el compilador la interpretación propia de la plataforma.

La creación de software es un proceso en múltiples etapas y hay cada vez más amenazas, como las que plantean los códigos malignos y las puertas traseras, que son imposibles de detectar con las herramientas de examen del código fuente, puesto que no son visibles en él. Esas amenazas pueden detectarse efectuando un análisis binario estático de la aplicación en su forma final.

De acuerdo con los requisitos y funcionalidades especificados en [UIT-T X.1524], las herramientas, repositorios y servicios utilizados para el análisis binario deben ser compatibles con la enumeración común de vulnerabilidades (CWE).

7.5 Prueba de penetración

Una prueba de penetración es un intento proactivo y autorizado de evaluar la seguridad de una infraestructura intentando explotar las vulnerabilidades del sistema, incluidos el sistema operativo (OS), el protocolo, los errores de aplicación, las configuraciones inadecuadas e incluso el comportamiento arriesgado del usuario extremo. El objetivo fundamental de la prueba de penetración es medir hasta qué punto es posible poner en peligro los sistemas o usuarios extremos y evaluar las consecuencias que de ello se desprende, como las incidencias que así puedan sufrir los recursos u operaciones implicados. Las pruebas suelen realizarse de manera manual o automática para poner sistemáticamente en peligro los servidores, los puntos extremos, las aplicaciones web, las redes inalámbricas, los dispositivos de red, los dispositivos móviles y otros posibles puntos de exposición. El objetivo de una prueba de penetración puede ser una caja blanca (que facilita información sobre el sistema y sus antecedentes) o una caja negra (que no facilita información o sólo información básica).

Al realizar una prueba de penetración, se pueden identificar proactivamente las vulnerabilidades más graves, las menos importantes y los falsos positivos, de manera que la organización pueda programar adecuadamente las medidas correctivas y aplicar los parches de seguridad necesarios.

De acuerdo con los requisitos y funcionalidades especificados en [UIT-T X.1544], las herramientas, repositorios y servicios utilizados para une prueba de penetración deben ser compatibles con la Enumeración y clasificación de pautas de ataques comunes (CAPEC).

Apéndice I

Diagrama de flujo

(Este apéndice no forma parte integrante de la presente Recomendación.)

Una buena manera de empezar el proceso de evaluación de la seguridad es organizar las técnicas de evaluación de la seguridad en un diagrama de flujo. Para ello puede considerarse el modelo en el que la evaluación se realiza desde la parte más elemental de la red hasta los sistemas integrados en la red. Se asegura en primer lugar el código fuente de los elementos de software, luego las aplicaciones y las bibliotecas del sistema, los sistemas de la red y por último la red en su globalidad.

Así, la evaluación global de la seguridad puede organizarse en dos grandes fases.

i) La primera es la fase previa al despliegue durante la cual puede verificarse en profundidad el objetivo utilizando todas las técnicas de evaluación de la seguridad presentadas y las conclusiones de esa evaluación se utilizarán para mitigar las vulnerabilidades encontradas.

ii) La segunda es la posterior al despliegue, cuando el objetivo ya está operativo en la red. En esta fase puede no resultar práctico someter al objetivo a todas las técnicas de evaluación, por lo que los analizadores de seguridad pueden realizar exploraciones de vulnerabilidades periódicas para asegurarse de que las vulnerabilidades identificadas tras el despliegue del producto se solucionan regularmente mediante la instalación de parches, etc.

En la fase previa al despliegue podrán analizarse en primer lugar los códigos fuente de los elementos de software para corregir los fallos detectados. Posteriormente se procesarán las aplicaciones y bibliotecas que utilizan mediante un análisis binario. A continuación se realizará la prueba de *fuzzing* y, por último, la exploración de vulnerabilidades y la prueba de penetración de los sistemas. Las conclusiones y observaciones de toda la evaluación se comunicarán a los creadores que corresponda a fin de que puedan aplicar las medidas correctivas necesarias para solventar todas las vulnerabilidades detectadas.

En la fase posterior al despliegue, toda la red podrá someterse periódicamente a una exploración de vulnerabilidades. Las vulnerabilidades deberán resolverse a medida que se vayan encontrando.

En la Figura 1.1 puede verse un diagrama de flujo del proceso expuesto.

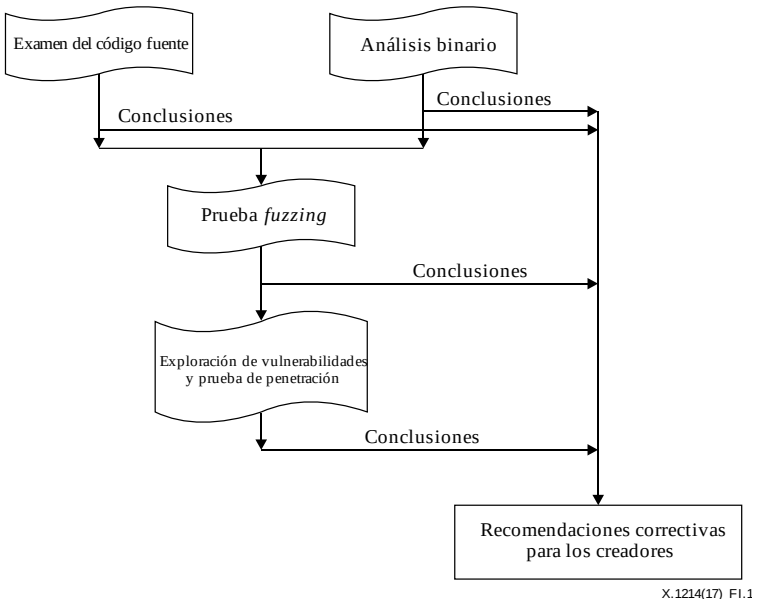

Figura I.1 – Diagrama de flujo de las técnicas de evaluación de la seguridad

Apéndice II

Técnicas suplementarias para aumentar la seguridad de una red de TIC

(Este apéndice no forma parte integrante de la presente Recomendación.)

En el presente Apéndice se presentan algunas técnicas que aumentan la seguridad de las redes de telecomunicaciones/TIC.

II.1 Evaluación de la solidez de las contraseñas

La autentificación por contraseñas se utiliza mucho en las redes de telecomunicaciones/TIC con fines como la configuración, la gestión, la operación y el mantenimiento y la prestación del servicio. Los administradores de sistema deben evaluar la robustez de esas contraseñas para asegurarse de que no se pueden piratear con facilidad. Para ello puede realizarse un desciframiento de contraseñas, para lo que existen varios mecanismos, como el ataque de diccionario, el ataque de fuerza bruta y los cuadros arco iris.

II.2 Evaluación de la confidencialidad social

En ocasiones se manipula psicológicamente a los empleados de las organizaciones para que divulguen información confidencial. Se trata de una estafa por confianza cuyo objetivo es obtener información, perpetrar un fraude o acceder a un sistema. Es posible recurrir a la ingeniería social para evaluar la credibilidad de esas personas o grupos dentro de la organización. Se pueden identificar objetivos específicos cuando la organización sabe que hay una amenaza o considera que la divulgación de información por parte de un individuo o grupo de individuos podría tener consecuencias graves.

II.3 Evaluación de la seguridad funcional

Aunque no se dispone de herramientas específicas para probar la seguridad funcional, este método suplementa las técnicas de detección de vulnerabilidades expuestas en las cláusulas II.1 y II.2.

Los requisitos de seguridad funcional de todo dispositivo/elemento de red utilizado en una red de telecomunicaciones/TIC son los siguientes:

i) autentificación local del usuario para la configuración y la gestión del dispositivo;

ii) autentificación a distancia del usuario para la configuración y la gestión del dispositivo;

iii) almacenamiento seguro de las contraseñas en el dispositivo;

iv) verificación de la gestión segura de claves criptográficas;

v) mecanismo de protección del dispositivo contra parches de software ilícitos;

vi) protección a distancia del tráfico de gestión del dispositivo;

vii) clasificación de los usuarios gestores del dispositivo en función de sus privilegios/permisos;

viii) sincronización temporal segura;

ix) generación de eventos (registros) de auditoría por el dispositivo sometido a prueba (DUT);

x) exportación segura de los registros de auditoría por el DUT.

II.4 Exploración inalámbrica

Los exploradores inalámbricos pueden ayudar a las organizaciones a tomar medidas correctivas para mitigar los riesgos de seguridad que plantean las tecnologías inalámbricas. Las herramientas de exploración inalámbrica deben poder explorar todos los dispositivos inalámbricos IEEE 802.11 [b-IEEE Std. 8802-11], ya sea a nivel nacional o internacional. Mediante la exploración inalámbrica pueden detectarse los dispositivos inalámbricos no autorizados que se encuentren en el radio de

acción de los exploradores, señales inalámbricas fuera del perímetro de una organización y las posibles puertas traseras o violaciones a la seguridad.

II.5 Utilización de módulos y algoritmos criptográficos seguros

Los algoritmos criptográficos se utilizan para la encriptación y desencriptación de datos de autentificación o usuario para la transferencia segura de los datos a través de las redes de telecomunicaciones/TIC. Aunque los algoritmos criptográficos estén bien diseñados, suele haber errores en su aplicación. Si se implantan en las redes de telecomunicaciones/TIC algoritmos inseguros con errores de aplicación, éstos pueden ser explotados por un pirata y causar graves pérdidas de datos o dar lugar a intrusiones fraudulentas. Así conviene utilizar en las redes de telecomunicaciones/TIC módulos y algoritmos criptográficos muy seguros.

II.6 Rastreo de la red

El rastreo de la red es una técnica pasiva que supervise la comunicación de la red, descodifica los protocolos y examina los encabezamientos para marcar la información interesante. También se denomina supervisión de la red o análisis de red y los administradores de redes o sistemas pueden legítimamente utilizarlo para supervisar el tráfico de red y solucionar eventuales problemas.

Con la información obtenida por el rastreador de red el administrador o experto en seguridad puede identificar los paquetes erróneos y utilizar los datos para detectar atascos y mantener la seguridad y la eficacia de la transmisión de datos en la red.

Bibliografía

[b-IEEE Std. 8802-11] ISO/IEC/IEEE 8802-11:2018(E) – *ISO/IEC/IEEE – International Standard – Information technology –Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications*

[b-CVE] CVE Numbering Authorities (1999-2018*). Common vulnerabilities and exposures list.* Mitre Corporation.
https://cve.mitre.org/cve/

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisiones de señales radiofónicas, de televisión y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y de otros elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la red de gestión de las telecomunicaciones y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para las transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	Conmutación y señalización, y mediciones y pruebas asociadas
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios telegráficos
Serie T	Terminales para servicios telemáticos
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos, comunicaciones de sistemas abiertos y seguridad**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet, redes de próxima generación, Internet de las cosas y ciudades inteligentes
Serie Z	Lenguajes y aspectos generales de soporte lógico para los sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2019