Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1544

(04/2013)

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

Intercambio de información de ciberseguridad – Intercambio de eventos/incidentes/eurística

Enumeración y clasificación de pautas de ataques comunes

Recomendación UIT-T X.1544

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	
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	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	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339
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/eurística	**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

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

Recomendación UIT-T X.1544

Enumeración y clasificación de pautas de ataques comunes

Resumen

La Recomendación UIT-T X.1544 es una especificación basada en XML/XSD para la identificación, descripción y enumeración de pautas de ataques. Las pautas de ataques son un mecanismo poderoso para detectar y comunicar el talante de los atacantes. Son descripciones de métodos comunes para la ejecución de programas informáticos. Se derivan del concepto de pautas de diseño en un contexto destructivo en lugar de constructivo y se generan a partir de un profundo análisis de ejemplos concretos del mundo real. El objetivo de la enumeración y clasificación de partes de ataques comunes (CAPEC) es proporcionar un catálogo de pautas de ataques de libre disposición junto con un sistema de clasificación.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio
1.0	ITU-T X.1544	2013-04-26	17

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

La Recomendación sobre enumeración y clasificación de pautas de ataques comunes (CAPEC) es una especificación basada en XML/XSD para la identificación, descripción y enumeración de pautas de ataques. Las pautas de ataques son un mecanismo poderoso para detectar y comunicar el talante de los atacantes. Son descripciones de métodos comunes para ejecutar programas informáticos. Se derivan del concepto de pautas de diseño en un contexto destructivo en lugar de constructivo y se generan a partir de un profundo análisis de ejemplos concretos del mundo real. El objetivo de CAPEC es proporcionar un catálogo de pautas de ataques de libre disposición junto con un sistema de clasificación.

Las CAPEC permiten:

- la normalización de la captura y descripción de las pautas de ataques;
- la recopilación de pautas de ataques conocidas en una enumeración integrada que la sociedad pueda aprovechar de forma completa y eficiente;
- la clasificación de las pautas de ataques de forma que los usuarios puedan identificar con facilidad el subconjunto de la enumeración que les resulte adecuado en su contexto;
- la vinculación, mediante referencias explícitas, entre las pautas de ataques y la enumeración de las debilidades comunes que las permiten.

La Recomendación UIT-T X.1544 se ha elaborado teniendo en cuenta la importancia de mantener, siempre que sea posible, la compatibilidad técnica con los "Requisitos y Recomendaciones para la compatibilidad CAPEC", versión 1.0, publicada por MITRE Corporation el 30 de agosto de 2012 [https://capec.mitre.org/compatible/requirements_v1.0.html].

Recomendación UIT-T X.1544

Enumeración y clasificación de pautas de ataques comunes

1 Alcance

La presente Recomendación facilita un intercambio estructurado de las pautas de ataques disponibles públicamente, junto a un esquema y un sistema de clasificación completos.

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.1500] Recomendación UIT-T X.1500 (2011), *Aspectos generales del intercambio de información de ciberseguridad (CYBEX).*

3 Definiciones

3.1 Términos definidos en otros documentos

Esta Recomendación utiliza los siguientes términos definidos en otros documentos:

3.1.1 autoridad de revisión [b-UIT-T X.1520]: Cualquier entidad que realice una revisión.

NOTA – Actualmente MITRE es la única autoridad de revisión.

3.1.2 vulnerabilidad [UIT-T X.1500]: Una debilidad en el software que podría ser utilizada para violar un sistema o la información que contiene.

3.2 Términos definidos en esta Recomendación

En esta Recomendación se definen los términos siguientes:

3.2.1 porcentaje de exactitud: Porcentaje de elementos de seguridad de la muestra de revisión que hacen referencia a los identificadores CAPEC correctos.

3.2.2 instancia de ataques: Ataque pormenorizado concreto contra una aplicación o sistema que busca vulnerabilidades o debilidades en ese sistema.

3.2.3 pauta de ataques: Abstracción de planteamientos de ataques comunes observados en el mundo contra aplicaciones o sistemas (por ejemplo, inyección SQL, de intermediarios, robo de sesión, etc.).

NOTA – Una sola pauta de ataque puede tener potencialmente muchas instancias de ataque variables asociadas a ella.

3.2.4 capacidad: Herramienta de evaluación, herramienta de pruebas de seguridad de aplicación dinámica (DAST), herramienta de pruebas de penetración, herramienta de modelización de amenazas, base de datos, sitio web, recomendación o servicio de seguridad que proporciona información sobre instancias y pautas de ataques.

3.2.5 mapa/correspondencia: Especificación de las relaciones entre elementos de pautas de ataques en un repositorio y los elementos CAPEC relacionados con dichos elementos.

3.2.6 propietario [basado en b-UIT-T X.1520]: Propietario (persona física o empresa) quien tiene la responsabilidad de la capacidad (definida en esta Recomendación).

3.2.7 repositorio: Conjunto implícito o explícito de elementos de pautas de ataques que soporta una capacidad, por ejemplo, una base de datos de pautas de ataques, el conjunto de instancias de ataques en una herramienta DAST o un sitio web.

3.2.8 revisión: Proceso para determinar si una capacidad es compatible con la CAPEC.

3.2.9 versión de revisión: Versión fechada de CAPEC utilizada para determinar la compatibilidad CAPEC de una capacidad.

3.2.10 elemento de seguridad: Registro de base de datos, sonda de evaluación, instancia de ataques, explotación, carga de pago, etc., relacionada con una pauta de ataques específica.

3.2.11 tarea: Sonda, verificación, firma, etc., de una herramienta que realiza una acción que genera información de seguridad (es decir, el elemento de seguridad).

3.2.12 herramienta: Programa informático o dispositivo que examina las propiedades de seguridad de una aplicación o sistema mediante la simulación, emulación o caracterización de posibles ataques contra dicho sistema, por ejemplo, herramienta de evaluación, herramienta de pruebas de seguridad de aplicación dinámica (DAST), herramienta de pruebas de penetración, herramienta de marco de explotación, herramienta de modelización de amenazas.

3.2.13 usuario [basado en b-UIT-T X.1520]: Consumidor o potencial consumidor de la capacidad (definida en esta Recomendación).

3.2.14 debilidad: Defecto o imperfección en el código, diseño, arquitectura o despliegue de un programa informático que podría, en algún momento, convertirse en una vulnerabilidad o que podría contribuir a la introducción de otras vulnerabilidades.

4 Abreviaturas y acrónimos

Esta Recomendación utiliza las abreviaturas y acrónimos siguientes:

CAPEC Enumeración y clasificación de pautas de ataque comunes *(common attack pattern enumeration and classification)*

CCR Representación de reclamación de cobertura (*coverage claim representation*)

CIA Confidencialidad, integridad o disponibilidad (*confidentially, integrity or availability*)

CWE Enumeración de debilidades comunes *(common weakness enumeration)*

DAST Herramienta de pruebas de seguridad de aplicación dinámica (*dynamic application security testing tool*)

GUI Interfaz de usuario gráfica *(graphical user interface)*

IDS Sistema de detección de intrusiones (*intrusion detection system*)

POC Punto de contacto *(point of contact)*

5 Convenios

En esta Recomendación los términos "requerido", "debe", "no debe", "debería", "no debería", "recomendado", "puede" y "facultativo" se emplean conforme a la guía de estilo del UIT-T. (Disponible en http://www.itu.int/oth/T0A0F000004/en).

6 Requisitos de alto nivel

Los elementos siguientes definen los conceptos, papeles y responsabilidades relativos a la utilización adecuada de identificadores CAPEC para que distintas capacidades destinadas a combatir las vulnerabilidades (herramientas, repositorios y servicios) puedan compartir datos con el fin de permitir la utilización común de bases de datos de vulnerabilidades y otras capacidades y facilitar el uso compartido de herramientas y servicios de seguridad.

Prerrequisitos

6.1 El propietario de la capacidad será una entidad legalmente válida, es decir, una organización o un individuo concreto con un número de teléfono, dirección de correo electrónico y domicilio postal válidos.

6.2 La capacidad proporcionará valor o información adicional a la proporcionada en la CAPEC (es decir, nombre, descripción, referencias y la información sobre debilidades).

6.3 El propietario proporcionará a la autoridad de revisión un punto de contacto técnico cualificado para responder a cuestiones relacionadas con la correspondencia y cualquier funcionalidad de la capacidad relativa a CAPEC.

6.4 La capacidad estará disponible para el público o para un conjunto de consumidores en una versión productiva o pública.

6.5 Para la compatibilidad con CAPEC, el propietario de la capacidad proporcionará a la autoridad de revisión un "Formulario de evaluación de los requisitos de compatibilidad CAPEC" completo.

6.6 El propietario proporcionará a la autoridad de revisión acceso libre al repositorio para que pueda determinar si el repositorio satisface todos los requisitos de precisión de correspondencia asociados.

6.7 El propietario de la capacidad permitirá a la autoridad de revisión utilizar el repositorio para identificar pautas de ataques que deban añadirse a las CAPEC.

6.8 El propietario de la capacidad se comprometerá a cumplir todos los requisitos de compatibilidad obligatorios de las CAPEC, incluyendo los requisitos obligatorios para el tipo concreto de capacidad.

Funcionalidad

6.9 Para la compatibilidad con CAPEC, la capacidad permitirá a los usuarios localizar los elementos de seguridad utilizando los identificadores CAPEC ("Búsqueda por CAPEC").

6.10 Para la compatibilidad con CAPEC, cuando la capacidad presente elementos de seguridad al usuario, permitirá que éste obtenga los identificadores CAPEC asociados ("Salida de CAPEC").

6.11 Para la compatibilidad con CAPEC, la correspondencia de la capacidad vinculará con precisión elementos de seguridad con los identificadores CAPEC adecuados ("Precisión del mapeo").

6.12 Para la compatibilidad con CAPEC, la documentación de la capacidad describirá adecuadamente la CAPEC, la compatibilidad de la CAPEC y cómo se utiliza en la capacidad la funcionalidad relacionada con la CAPEC ("Documentación CAPEC").

6.13 Para la compatibilidad con CAPEC, la documentación de la capacidad disponible al público enumerará explícitamente los identificadores CAPEC que el propietario de la capacidad considere que cubren parte de su funcionalidad ("Cobertura CAPEC").

6.14 Para la compatibilidad con CAPEC, el sitio web de la capacidad disponible al público debería proporcionar la cobertura CAPEC de la capacidad como un documento o documentos XML de representación de reclamación de cobertura CAPEC (CCR).

6.15 La capacidad informará de su fecha de actualización CAPEC utilizada ("Fecha de uso").

6.16 La capacidad cumplirá cualquier requisito adicional para el tipo específico de capacidad, tal como se especifica en el Anexo A.

6.17 La capacidad cumplirá todos los requisitos de su medio de distribución, según se especifica en el Anexo B.

6.18 No se requiere que la capacidad haga lo siguiente:

- utilizar las mismas descripciones o referencias que la CAPEC;
- incluir cada identificador CAPEC en su repositorio.

Aspectos misceláneos

6.19 Si la capacidad no satisface todos los requisitos anteriores (cláusulas 6.1 a 6.18), el propietario no la anunciará como compatible con CAPEC.

7 Exactitud

La compatibilidad con CAPEC sólo permite el intercambio de datos si la correspondencia de la capacidad es exacta. Por tanto, las capacidades compatibles con CAPEC deben satisfacer los requisitos mínimos de exactitud siguientes.

7.1 El repositorio tendrá un nivel de exactitud del 100%.

7.2 Durante el periodo de revisión, el propietario de la capacidad corregirá cualquier error de correspondencia que detecte la autoridad de revisión.

7.3 Después del periodo de revisión, el propietario debería corregir cualquier error de correspondencia identificado tras un tiempo razonable desde que informó del mismo, es decir, en las siguientes dos (2) versiones del repositorio o seis (6) meses, eligiendo el más corto.

7.4 El propietario debería elaborar y firmar una declaración en la que, hasta donde alcance su conocimiento, se afirme que la correspondencia no tiene errores.

7.5 Si la capacidad está basada o utiliza otra capacidad compatible con CAPEC (la capacidad "fuente"), y el propietario de la capacidad es consciente de errores de correspondencia en la capacidad fuente, el propietario informará de dichos errores al propietario de la capacidad fuente.

8 Documentación

La documentación que se proporciona con la capacidad debe cumplir los requisitos siguientes.

8.1 La documentación incluirá una breve descripción de la CAPEC y de la compatibilidad de la CAPEC, que puede estar basada en extractos literales de documentos del sitio web de la CAPEC.

8.2 La documentación describirá cómo puede encontrar el usuario elementos de seguridad individuales en el repositorio de la capacidad utilizando identificadores CAPEC.

8.3 La documentación describirá cómo puede el usuario obtener identificadores CAPEC de elementos individuales en el repositorio de la capacidad.

8.4 Si la documentación incluye un índice, éste debería incluir referencias a la documentación asociada a la CAPEC bajo el término "CAPEC."

9 Fecha de uso de la CAPEC

Los usuarios deben conocer qué versión de CAPEC se utiliza en un repositorio de una capacidad en lo que respecta a su correspondencia con CAPEC. El propietario de la capacidad pude indicar la vigencia de la correspondencia proporcionando la versión de la CAPEC o la fecha de la última actualización de la correspondencia.

9.1 Cada nueva versión de la capacidad identificará la versión o fecha de actualización más reciente de la CAPEC utilizada para crear o actualizar la correspondencia mediante al menos uno de los mecanismos siguientes: cambio de registros de acceso, listas de nuevas características, ficheros de ayuda u otro mecanismo. La capacidad se considera "actualizada" con respecto a dicha versión o fecha de actualización.

9.2 Cada nueva versión de la capacidad debería estar actualizada en relación con la versión de CAPEC declarada que no sea anterior en más de cuatro (4) meses a la disponibilidad de la capacidad para los usuarios. Si una capacidad no satisface este requisito se considera que está "desactualizada".

9.3 El propietario de la capacidad hará pública la frecuencia con que actualizará el repositorio de la capacidad en cuanto esté disponible una nueva versión o actualización de la CAPEC en el sitio web de la CAPEC.

10 Revocación de la compatibilidad CAPEC

10.1 Si una autoridad de revisión ha verificado que una capacidad es compatible con CAPEC, pero ulteriormente tiene evidencias de que no se cumplen los requisitos, la autoridad de revisión puede revocar su aprobación.

10.1.1 La autoridad de revisión identificará los requisitos específicos que no se cumplen.

10.2 La autoridad de revisión determinará si las acciones o reclamaciones del propietario son "deliberadamente equivocadas".

10.2.1 La autoridad de revisión puede interpretar la expresión "deliberadamente equivocadas" como considere oportuno.

10.3 La autoridad de revisión no debería considerar la revocación de la compatibilidad CAPEC para una capacidad determinada en más de una ocasión cada seis (6) meses.

Aviso y evaluación

10.4 La autoridad de revisión proporcionará al propietario de la capacidad y al punto de contacto (POC) técnico un aviso de revocación al menos dos (2) meses antes de la fecha en que esté prevista la revocación.

10.4.1 Si la autoridad de revisión concluye que las actuaciones o reclamaciones del propietario son deliberadamente equivocadas, puede obviar el periodo de aviso.

10.5 Si el propietario de la capacidad considera que se cumplen los requisitos, puede responder al aviso de revocación proporcionando información que demuestre porqué la capacidad cumple los requisitos que han sido cuestionados.

10.6 Si durante el periodo de aviso el propietario modifica la capacidad para que cumpla los requisitos cuestionados, la autoridad de revisión debería finalizar la actuación de revocación de dicha capacidad.

Revocación

10.7 La autoridad de revisión puede retrasar la fecha de revocación.

10.8 La autoridad de revisión hará pública la revocación de compatibilidad CAPEC para dicha capacidad.

10.9 Si la autoridad de revisión concluye que las actuaciones del propietario de la capacidad en relación con los requisitos de compatibilidad de la CAPEC son deliberadamente equivocadas, la revocación debería estar vigente al menos un año.

10.10 La autoridad de revisión podrá hacer públicas las razones de una revocación.

10.11 El propietario de la capacidad puede presentar en el mismo sitio una declaración pública relativa a la revocación.

10.12 Si se revoca la aprobación, el propietario NO podrá solicitar una nueva revisión durante el periodo de revocación.

11 Autoridad de revisión

11.1 La autoridad de revisión analizará la compatibilidad CAPEC en relación con una versión concreta de la CAPEC, la versión de revisión.

11.2 La autoridad de revisión identificará claramente la versión de revisión utilizada para establecer la compatibilidad de la capacidad.

11.3 La autoridad de revisión identificará claramente la versión del documento de requisitos de compatibilidad de la CAPEC utilizado para establecer la compatibilidad de la capacidad.

11.4 La autoridad de revisión analizará cada elemento del repositorio de la capacidad para determinar la precisión de la correspondencia.

11.5 La autoridad de revisión debería analizar cada capacidad por lo menos una vez al año para determinar su precisión de correspondencia.

11.6 La autoridad de revisión proporcionará una copia del formulario de declaración de compatibilidad de la CAPEC a solicitud de todo propietario de capacidad válido que desee iniciar el proceso de compatibilidad de la CAPEC.

11.7 La autoridad de revisión proporcionará una copia del formulario de evaluación de los requisitos de compatibilidad de la CAPEC a solicitud de todo propietario de capacidad que haya presentado un formulario de declaración de compatibilidad de la CAPEC completo.

Anexo A

Requisitos específicos de los tipos de capacidades

(Este anexo forma parte integral de la presente Recomendación.)

Dado que existe una amplia variedad de capacidades que utilizan la CAPEC, algunos tipos de capacidades pueden tener características singulares que precisen una atención especial en relación con la compatibilidad CAPEC.

A.1 La capacidad cumplirá todos los requisitos adicionales relacionados con el tipo específico de capacidad.

A.1.1 Si la capacidad es una herramienta de evaluación, una herramienta de pruebas de seguridad de aplicación dinámica (DAST), una herramienta de pruebas de penetración, una herramienta de marco de explotación, una herramienta de modelización de amenazas o un producto que integre los resultados de uno o más de estos elementos, debe satisfacer los apartados de los Requisitos de las herramientas A.2.1 a A.2.8.

A.1.2 Si la capacidad es un servicio (por ejemplo, un servicio de evaluación de seguridad, un servicio de pruebas de penetración o un servicio de enseñanza o formación) debe satisfacer los apartados de los requisitos de los servicios de seguridad A.3.1 a A.3.5.

A.1.3 Si la capacidad es una base de datos de ataques conocidos en línea, un recurso basado en la red o un sitio para información debe satisfacer los apartados de los requisitos de las capacidades en línea A.4.1 a A.4.3.

A.2 Requisitos de las herramientas

A.2.1 La herramienta permitirá al usuario utilizar los identificadores CAPEC para localizar tareas asociadas en dicha herramienta ("Búsqueda por CAPEC") proporcionando al menos uno de los mecanismos siguientes: función "buscar" o "encontrar", correspondencia entre dichos nombres de tareas de herramientas y los identificadores CAPEC, u otro mecanismo que la autoridad de revisión considere suficiente.

A.2.2 Para cualquier informe que identifique elementos de seguridad individuales, la herramienta permitirá al usuario determinar los identificadores CAPEC asociados a dichos elementos ("Salida por CAPEC") mediante al menos uno de los mecanismos siguientes: inclusión de identificadores CAPEC directamente en el informe, correspondencia entre dichos nombres de tareas de herramientas y los identificadores CAPEC u otro mecanismo que la autoridad de revisión considere suficiente.

A.2.3 La documentación disponible al público enumerará explícitamente los identificadores CAPEC que el propietario de la capacidad considere una herramienta eficaz para las instancias ("cobertura de reclamación de compatibilidad CAPEC").

A.2.4 El sitio web de la capacidad disponible al público puede proporcionar la cobertura de reclamación de compatibilidad CAPEC como un documento o documentos XML de representación de reclamación de cobertura CAPEC (CCR).

A.2.5 Cualquier informe o correspondencia que sea necesaria satisfará los requisitos de medios especificados en el Anexo B.

A.2.6 La herramienta, o el propietario de la capacidad, deberían proporcionar al usuario una lista con todos los identificadores CAPEC asociados con las tareas de la herramienta.

A.2.7 La herramienta debería permitir al usuario seleccionar un conjunto de tareas proporcionando un fichero que contenga una lista de identificadores CAPEC.

A.2.8 La interfaz de la herramienta debería permitir al usuario visualizar, seleccionar y descartar un conjunto de tareas utilizando identificadores CAPEC individuales.

A.2.9 Si la herramienta no tiene una tarea que esté asociada con un identificador CAPEC tal como haya especificado el usuario en los requisitos de herramienta apartado A.2.5 o apartado A.2.6, la herramienta debería notificar al usuario que no puede realizar la tarea asociada.

A.3 Requisitos de los servicios de seguridad

Los servicios de seguridad pueden utilizar en su actividad herramientas compatibles con CAPEC, pero pueden no ofrecer a sus clientes acceso directo a dichas herramientas. Por tanto, puede resultar difícil a los clientes identificar y comparar las capacidades de distintos servicios. Los Requisitos de los servicios de seguridad abordan esta potencial limitación.

A.3.1 El servicio de seguridad deberá poder utilizar identificadores CAPEC para indicar al usuario qué elementos de seguridad ha probado o detectado el servicio ("Búsqueda por CAPEC") mediante uno o más de los mecanismos siguientes: proporcionar al usuario una lista de identificadores CAPEC que identifiquen los elementos probados o detectados por el servicio, proporcionar al usuario una correspondencia entre los elementos del servicio y los identificadores CAPEC, responder a una lista de identificadores CAPEC facilitada por un usuario con la indicación de qué indicadores han sido probados o detectados por el servicio, o utilizar cualquier otro mecanismo.

A.3.2 Para cualquier informe que identifique elementos de seguridad individuales, el servicio permitirá al usuario determinar los indicadores CAPEC asociados a dichos elementos ("Salida por CAPEC) mediante uno o más de los mecanismos siguientes: permitir al usuario incluir indicadores CAPEC directamente en el informe, proporcionar al usuario la correspondencia entre los elementos de seguridad y los indicadores CAPEC, o utilizar cualquier otro mecanismo.

A.3.3 La documentación disponible al público enumerará explícitamente los identificadores CAPEC que el propietario de la capacidad considere como el servicio de seguridad que cubre adecuadamente su oferta ("cobertura de reclamación de compatibilidad CAPEC").

A.3.4 El sitio web de la capacidad disponible al público puede proporcionar la cobertura de reclamación de compatibilidad CAPEC como un documento o documentos XML de representación de reclamación de cobertura CAPEC (CCR).

A.3.5 Cualquier informe o correspondencia necesaria proporcionada por el servicio cumplirá los requisitos de medios especificados en el Anexo B.

A.3.6 Si el servicio proporciona al usuario acceso directo a un producto que identifique elementos de seguridad, el producto debería ser compatible con CAPEC.

A.4 Requisitos de las capacidades en línea

A.4.1 Una capacidad en línea permitirá a un usuario encontrar elementos de seguridad conexos en el repositorio de la capacidad en línea ("Búsqueda por CAPEC") mediante uno de los mecanismos siguientes: una función de búsqueda que devuelva identificadores CAPEC para elementos conexos, una correspondencia que vincule cada elemento con su identificador o identificadores CAPEC asociados, o cualquier otro mecanismo.

A.4.1.1 La capacidad en línea debería proporcionar una "plantilla" de URL que permita a un programa informático construir fácilmente un enlace para acceder a la función de búsqueda, tal como se señala en el apartado A.4.1 sobre Requisitos de las capacidades en línea.

Ejemplos:

http://www.example.com/cgi-bin/db-search.cgi?capecid=XXX
http://www.example.com/capec/xxx.html

A.4.1.2 Si el sitio es de acceso público sin necesidad de registrarse, el programa debería aceptar el método "GET".

A.4.2 Para cualquier informe que identifique elementos de seguridad individuales, la capacidad en línea permitirá al usuario determinar los identificadores CAPEC asociados para dichos elementos ("Salida por CAPEC") mediante al menos uno de los mecanismos siguientes: permitir al usuario incluir identificadores CAPEC directamente en el informe, proporcionar al usuario una correspondencia entre los elementos de seguridad y los identificadores CAPEC, o utilizar cualquier otro mecanismo.

A.4.3 La documentación disponible al público enumerará explícitamente los identificadores CAPEC que el propietario de la capacidad considere como el repositorio de la capacidad en línea adecuado ("cobertura de reclamación de compatibilidad CAPEC").

A.4.4 El sitio web de la capacidad disponible al público puede proporcionar la cobertura de reclamación de compatibilidad CAPEC como un documento o documentos XML de representación de reclamación de cobertura CAPEC (CCR).

A.4.5 Si la capacidad en línea no proporciona información detallada de los elementos de seguridad individuales, la capacidad en línea proporcionará una correspondencia que enlace cada elemento con su identificador o identificadores CAPEC asociados.

Anexo B

Requisitos de los medios

(Este anexo forma parte integral de la presente Recomendación.)

B.1 El medio de distribución utilizado por una capacidad compatible con CAPEC utilizará uno de los formatos de medios incluidos en este Anexo.

B.2 El formato de medios cumplirá los requisitos específicos de dicho formato.

B.3 Documentos electrónicos (HTML, procesador de texto, PDF, texto ASCII, etc.)

B.3.1 El documento estará escrito en un formato comúnmente disponible que tenga lectores con funciones de tipo "encontrar" o "buscar" ("Búsqueda por CAPEC"), tales como texto ASCII, HTML o PDF.

B.3.2 Si el documento solo proporciona nombres cortos o títulos para elementos individuales, enumerará los identificadores CAPEC relacionados con dichos elementos ("Salida por CAPEC").

B.3.3 El documento debería incluir una correspondencia entre elementos e identificadores CAPEC, que enumere las páginas de cada elemento.

B.4 Interfaz gráfica de usuario

B.4.1 La interfaz de usuario gráfica (GUI) proporcionará al usuario una función de búsqueda que le permita introducir un identificador CAPEC y recuperar los elementos conexos ("Búsqueda por CAPEC").

B.4.2 Si la GUI enumera la información detallada de un elemento individual, enumerará el identificador o identificadores CAPEC que se correspondan con dicho elemento ("Salida por CAPEC"). En cualquier otro caso, la GUI proporcionará al usuario una correspondencia en un formato que cumpla el requisito de documentos electrónicos señalado en B.3.1.

B.4.3 La GUI debería permitir al usuario exportar o acceder a datos relacionados con la CAPEC en un formato alternativo que cumpla el requisito de documentos electrónicos señalado en B.3.1.

Bibliografía

[b-UIT-T X.1520] Recomendación UIT-T X.1520 (2011), *Vulnerabilidades y exposiciones comunes.*

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios generales de tarificación
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 transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Terminales y métodos de evaluación subjetivos y objetivos
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
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 y Redes de la próxima generación
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2013