Análisis de la modelización de ataques para la seguridad en TIC

Prof. Dr. Javier Areitio Bertolín

Catedrático de la Facultad de Ingeniería ESIDE
Director del Grupo de Investigación Redes y Sistemas
Universidad de Deusto
E-Mail: jareitio@eside.deusto.es

En el presente artículo se propone y analiza un mecanismo para documentar ataques a las TIC (tecnologías de la Información y las Comunicaciones) de una forma estructurada y reutilizable. La ingeniería de seguridad opera con las TIC y necesita una forma adecuada de utilizar y analizar los datos de los ataques para poder aprender de las experiencias pasadas. La técnica que analiza el artículo es especialmente efectiva a la hora de valorar y gestionar los riesgos procedentes de adversarios inteligentes hostiles. Es útil para analizar amenazas contra todo tipo de activos como sistemas de información, infraestructura física-lógica, etc. La modelización que ofrecen los árboles de ataque proporciona soluciones de seguridad efectivas, económicas y decisiones de atenuación de riesgos útiles. Los árboles de ataque permiten crear un modelo gráfico estructurado en forma de árbol para describir los modos en que un sistema TIC puede ser comprometido o dañado.

Los gobiernos, empresas públicas y privadas, etc. han sido muy reticentes a la hora de divulgar sus ataques a sus sistemas TIC por temor a muy diversos motivos como por ejemplo perder la confianza y respeto depositada por sus clientes y el público en general, evitar que los ciber-atacantes exploten la misma o similar vulnerabilidad existente (utilizando el ocultismo), etc. Esto ha traído consigo una carencia de datos referentes a ataques disponibles públicamente. La ingeniería de seguridad de TIC debe utilizar los datos de fallos de seguridad (datos de un ataque concreto) existentes para poder mejorar sus diseños, implementaciones, asesoramientos, etc.

Algunos cambios significativos que han motivado que las amenazas hostiles a las TIC deban ser hoy en día consideradas seriamente por todo tipo de organizaciones poniendo recursos adecuados para tal fin son:

- La dependencia cada vez más extensa de la sociedad en TIC ha incrementado enormemente la cantidad de daño que puede ser producido potencialmente en los negocios y ciudadanos.
- La accesibilidad y familiaridad con TIC por parte de un colectivo creciente de personas ha aumentado significativamente el nivel de las amenazas.
- Los cambios en el orden mundial han dado lugar a un colectivo cada vez mayor de personas desinhibidas por las barreras morales, que están dispuestas y son capaces de producir daño en sistemas TIC por diferentes motivos económicos, psicológicos, etc.
- Cada vez mas los controles legislativos van pidiendo responsabilidades a las organizaciones en relación a brechas a su seguridad (por ejemplo, la Ley 34/2002 de 11 de Julio de Servicios de la Sociedad de la Información y de Comercio Electrónico (BOE nº 166 – 12/7/2002); la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (BOE nº 298 – 14/12/99); etc.).

Los árboles de ataque son técnicas que se derivan de las amenazas y ataques analíticos utilizados durante el análisis de los requisitos de seguridad. Aseguran que se desarrollen, completen, justifiquen y se encuentren bien documentados los requisitos de seguridad de un sistema. Toda organización normalmente posee un conjunto de árboles de ataque que son relevantes para su operación. La raíz de cada árbol incluye un evento que representa una forma de verse comprometida la seguridad o supervivencia de la empresa. La forma en que un atacante puede causar este compromiso se representa de forma iterativa e incremental como los nodos mas bajos del árbol. Un árbol de ataque puede representarse en diferente nivel de abstracción. La raíz del árbol representa un compromiso de la seguridad o un evento que puede conducir a verse comprometida. Los otros nodos del árbol refinan de forma incremental e iterativa el compromiso representado por la raíz.

Árboles de ataque. Representaciones. Escenarios de intrusión. Refinamiento ataques. Propiedad de transparencia referencial.

Los árboles de ataque representan un método sistemático de caracterizar la seguridad de los sistemas, refinan la información relativa a ataques identificando el compromiso de la seguridad o supervivencia de la empresa como la raíz del árbol. Los modos en que el atacante puede causar este compromiso se representan de forma iterativa y creciente como los nodos de nivel mas bajo del árbol.

Una empresa normalmente tiene un conjunto de árboles de ataque que son relevantes a sus operaciones. La raíz de cada árbol representa un evento que puede dañar de forma significativa la misión de la empresa. Cada árbol de ataque enumera y elabora las formas en que un atacante puede causar que ocurra el evento. Cada camino a través de un árbol de ataque representa un único ataque a la empresa. Se puede descomponer (figura 1) un nodo de un árbol de ataque de dos formas:
(a) Un conjunto de sub-objetivos de ataque, todos los cuales se deben realizar para que tenga éxito el ataque, esto se representa como una descom posición “and”.
(b) Un conjunto de sub-objetivos de ataque, cualquiera de los cuales debe realizarse para que tenga éxito el ata que, esto se representa como una descomposición “or”.

Los árboles de ataque se pueden representar gráficamente o en forma de texto, figura 1. Los árboles de ataque constan de cualquier combinación de descomposiciones “and” y “or”. Se pueden generar escenarios de intrusión individuales a partir de un árbol de ataque según se indica en la figura 2. En general los objetivos de las hojas del árbol se añaden al final de los escenarios

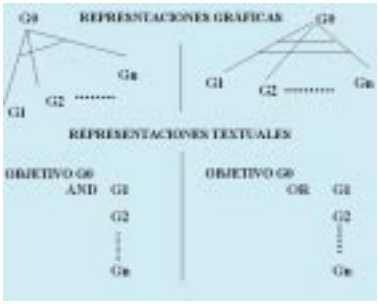

Figura. 1.- Dos formas de representar un árbol de ataque (gráfico y textual). Dos formas de descomponer un bloque en sub-bloques con las operaciones "and" y "or".

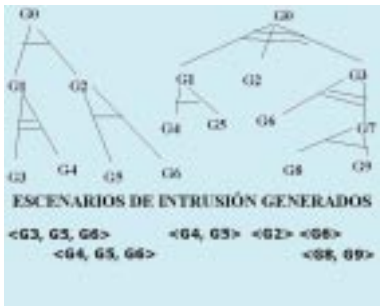

Figura 2.- Generación de Escenarios de Intrusión a partir de dos árboles de ataque

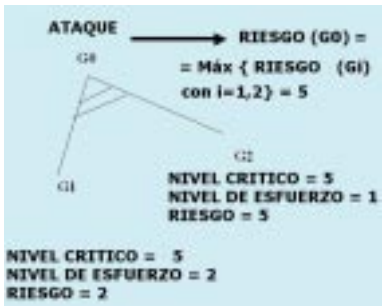

Figura 3.- Representación del cálculo del riesgo de un ataque G0.

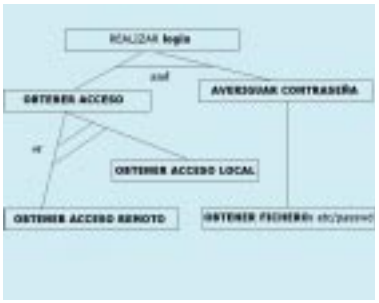

Figura 4.- Arbol de ataque que representa como un atacante puede leer el fichero donde residen los «hash» de las contraseñas: /etc/passwd en una computadora victima con S.O. Unix.

cuando se generan. Las descomposiciones "or" dan lugar a que se generen nuevos escenarios. Las descomposiciones "and" dan lugar a que los escenarios que existen se extiendan. Los nodos intermedios del árbol de ataque no aparecen en los escenarios de intrusión debido a que se elaboran con los objetivos de menor nivel.

Los árboles de ataque permiten el refinamiento de ataques a un nivel de detalle elegido por el desarrollador. Poseen la propiedad de transparencia referencial que implica que los detalles de nivel mas bajo relevantes de una entidad se abstraen en vez de omitir en un sistema particular de descripción de mayor nivel, de modo que la descomposición de nivel mayor contiene todo lo que se necesita para entender la entidad cuando se coloca en un contexto más grande.

Esta propiedad permite al desarrollador explorar ciertos caminos de ataque en mas profundidad que otros, mientras se permite al desarrollador generar escenarios de intrusión que tengan sentido. Además, el refinamiento de las ramas de un árbol de ataque genera nuevas ramas que dan lugar a escenarios de intrusión en un nuevo nivel de abstracción mas bajo.

Los árboles de ataque (a veces denominados árboles de fallos) se pueden utilizar para el análisis de condiciones de fallo de sistemas TIC complejos. Los árboles de ataque pueden capturar las etapas de un ataque y su interdependencia. Los árboles de ataque también se pueden utilizar para representar y calcular probabilidades, riesgos, costos, etc. Los principales bloques de construcción de los árboles de ataque son los nodos, estos pueden utilizarse para modificar las fases de un ataque o las acciones del atacante. Cada árbol tiene un único nodo superior raíz que representa el logro del objetivo último del ataque.

En el siguiente escenario simple de ataque el nodo raíz debería arrancar un "login shell" en la máquina de computación objetivo, figura 4. Las interdependencias de objetivos se modelizan por la jerarquía del árbol. Las etapas de ataque que se tienen que realizar con éxito antes de que otra etapa pueda ocurrir, se representan por medio de nodos "hijo". A cada nodo se asocia un operador lógico booleano binario "and" u "or". Para que un nodo con operador "and" ocurra es necesario que todos los eventos "hijo" ocurran. Los nodos del árbol de ataque pueden ser aumentados con probabilidades de ataque o costo para que se pueda calcular el camino de ataque menos caro o el mas probable.

El enfoque de los árboles de ataque presenta ciertas ventajas que lo hace una buena elección para representar el conocimiento de ataques gestionado de forma cooperativa. La estructura jerárquica puede simplificar la navegación y permite que varios ingenieros de seguridad puedan trabajar en diferentes ramas del árbol en paralelo. El concepto de árbol de ataque es fácil de entender, permite un rango mayor de personas que saquen ventaja de un árbol de ataque o contribuyan a ello.

La figura 4 se refiere a un atacante que ha encontrado una forma de leer el fichero /etc/passwd de una máquina de computación con sistema operativo Unix. El fichero contiene los "hash" (ó resúmenes, tras pasar por una función criptográfica unidireccional como MD5 ´0 SHA1) de las contraseñas (no se utilizarán "shadow passwords") y un usuario ha elegido una contraseña débil (por ejemplo muy corta menos de 8 caracteres con caracteres sólo alfabéticos), esto permite al atacante averiguar por fuerza bruta la contraseña de ese usuario y abrir sesión en la computadora con los privilegios de ese usuario insensato.

Esta descripción informal de ataque contiene diferentes informaciones:
(a) Etapas del ataque y su orden en el tiempo. La primera etapa es obtener el fichero /etc/passwd, luego averiguar la contraseña con éxito y finalmente abrir sesión (ó "login") en la maquina de computación.
(b) Interdependencias de las etapas del ataque. El análisis con éxito de la contraseña es posible si el contenido del fichero /etc/passwd se conoce y contiene los "hash" de contraseñas y un usuario insensato ha elegido una contraseña débil.

(c) Precondiciones de un ataque. La habilidad del atacante para leer el fichero /etc/passwd y la existencia de una contraseña débil.
(d) Postcondiciones del ataque. Cuando el atacante entra en la computadora, obtiene nuevos privilegios y capacidades (por ejemplo, instalar una "puerta trasera" para acceder cuando lo desee o un "troyano" que fugue información de forma no advertida por nadie).
(e) Acciones del atacante. Alguna acción debe realizar el atacante para obtener el conocimiento del fichero /etc/passwd para conocer una contraseña (la más débil).
(f) Capacidades y recursos necesarios. Para averiguar una contraseña por "fuerza bruta" con éxito el atacante necesita suficiente potencia de computación o un buen diccionario de criptoanálisis.

Determinación cuantitativa del riesgo. Metodo-proceso para valorar riesgos

Los riesgos pueden evaluarse estimando dos factores para cada nodo de un árbol de ataque:
(a) Nivel de esfuerzo requerido por un atacante para llevar a cabo una amenaza dada.
(b) Nivel de crítico de que los activos del sistema sean expuestos al ataque.

El riesgo se puede calcular dividiendo el nivel de crítico entre el nivel de esfuerzo. La estimación en un nodo dado puede derivarse utilizando la estimación en sus sub-nodos y sus conexiones lógicas. La figura 3 muestra como calcular el riesgo de un ataque G0. La estimación del nivel de crítico o de esfuerzo se puede obtener combinando el consenso de expertos con evidencia de campo y test disponibles. Una alternativa común consiste en utilizar estimaciones cualitativas empleando tasas como: alto, bajo, moderado, etc. Para valorar riesgos basándose en el árbol de ataques se puede seguir el siguiente método-proceso de cinco pasos:
(1) Crear un árbol de ataque que muestra las posibles formas de atacar un sistema TIC.
(2) Predecir de que forma los adversarios atacarán (si alguien tiene motivación para cometer un acto hostil y dispone de todas las capacidades (dinero, adiestramiento, recursos, deseo de aceptar las consecuencias, etc) entonces se puede esperar razonablemente que ataque.

$$PE = AF \cdot V$$

Donde: PE = Probabilidad del evento
AF = Amenaza-frecuencia
V = Vulnerabilidad
Así mismo:

$$R = A \cdot V \cdot DR$$

Donde: R = Riesgo
A = (Amenaza)
V = (Vulnerabilidad)
DR = (Daño resultante)
(3) Identificar el impacto asociado con cada escenario de ataque. Un escenario de ataque es el conjunto de eventos que caracteriza un ataque concreto.
(4) Determinar el nivel de riesgo asociado con cada escenario de ataque.
(5) Monitorizar el sistema en busca de signos de que un escenario de ataque esta en progreso.

Patrones de ataque. Reutilización. Perfiles de ataque. Buffer-overflow

Lo práctico de los árboles de ataque para caracterizar ataques en los sistemas del mundo real depende de su capacidad de reutilizar patrones de ataque desarrollados anteriormente. Dos estructuras que soportan dicha reutilización son:
- Un patrón de ataque para caracterizar un tipo individual de ataque.
- Un perfil de ataque para organizar los patrones de ataque para hacer más fácil buscarlos y aplicarlos.

Se define un "patrón de ataque" como una representación genérica de un ataque malicioso deliberado que ocurre comúnmente en contextos específicos. Cada patrón de ataque contiene:
(a) Un objetivo global del ataque especificado por el patrón.
(b) Una lista de pre-condiciones para su uso.
(c) Las etapas para realizar el ataque.
(d) Una lista de post-condiciones que son ciertas si tiene éxito el ataque.

Las pre-condiciones son suposiciones que se realizan acerca del atacante o el estado de la empresa que son necesarias para que tenga éxito un ataque. Ejemplos de pre-condiciones son las habilidades-técnicas, recursos, acceso o conocimiento que debe poseer el atacante y el nivel de riesgo que se debe estar dispuesto tolerar. Las post-condiciones son el conocimiento ganado por el atacante y los cambios en el estado de la empresa que resultan de llevar a cabo con éxito las etapas del ataque cuando se mantienen las pre-condiciones.

En la pasada década una de las formas mas comunes de vulnerabilidad de seguridad ha sido la gestión incorrecta del "buffer overflow" por los programas informáticos. Cuando un programa se llama se añade a la pila de ejecución del sistema un registro de activación. Cada registro de activación contiene la dirección de vuelta cuando termina el programa y cualquier variable y buffers locales. En ciertos programas la entrada de usuario excesivamente larga puede causar que se satura el buffer interno. La saturación del buffer ó "buffer overflow" puede re-escribir las variables locales, el puntero de retorno y otras porciones de la memoria adyacente. Un atacante puede, por tanto, construir la entrada de usuario para cambiar el puntero de retorno para volver a una zona de código malicioso a elección del atacante. Este código malicioso se ejecuta al volver con los privilegios del programa original. Si el programa se ejecuta con privilegios de administrador, que frecuentemente es el caso, el atacante en esencia tiene el control completo del sistema.

Petición de ataque de "buffer overflow"

Objetivo:
Explotar la vulnerabilidad del "buffer overflow" para realizar una función maliciosa en el sistema destino

Precondiciones:
El atacante puede ejecutar ciertos programas en el sistema destino.

Ataque:
and
1) Identificar el programa ejecutable en el sistema destino susceptible de la vulnerabilidad "buffer overflow".
2) Identificar el código que realizará la función maliciosa cuando se ejecute con los privilegios del programa original.
3) Construir el valor de entrada que fuerza que el código este en el espacio de direcciones del programa.
4) Ejecutar el programa de forma que haga saltar a la dirección en la que reside el código.

Post-condiciones:
El sistema destino realiza una función maliciosa.

Cuadro 1

Este patrón de ataque se captura como se muestra en el cuadro 1.

Los patrones de ataque se pueden organizar en un perfil de ataque que los abarca. Los perfiles de ataque contienen:
(a) Un modelo de referencia común.
(b) Un conjunto de variantes.
(c) Un conjunto de patrones de ataque.
(d) Un glosario de términos y frases definidas.

El modelo de referencia representa una plantilla de arquitectura con parámetros que puede incluir variantes específicas. Los patrones de ataque también se definen en términos de las variantes. Los perfiles de ataque se especifican independientemente de cualquier empresa concreta. Una empresa cuya arquitectura sea consistente con un modelo de referencia de perfil puede utilizar los patrones de ataque del perfil, una vez instanciados para ayuda a construir árboles de ataque relevantes a la operación de la empresa. Los perfiles de ataque diferentes pueden direccionar diferentes niveles de acceso del atacante, recursos y habilidades así como diferentes configuraciones de componentes del sistema. Por tanto, los perfiles de ataque diferentes pueden ayudar a refinar un árbol de ataque de una empresa específica a lo largo de diferentes líneas de ataque.

Caso práctico: Árbol de ataque de una organización

Describamos a continuación un árbol de ataque de alto nivel donde el nodo raíz representa la revelación de secretos de propiedad intelectual de una organización. Se incluyen todos los posibles tipos de ataques: ingeniería social, acceso físico y tecnológicos (ver cuadro 2).

La primera rama en la descomposición de alto nivel "OR" trata de los ataques denominados "revisar basuras" tanto dentro de la organización utilizando el servicio de limpieza fraudulento o después de que las basuras hayan salido de la organización (es útil trituradoras de papeles y borradores de bajo nivel para soportes de información disquetes, discos duros, etc.).

La segunda rama del árbol de ataque trata de los ataques basados en las emanaciones de monitores (electromagnéticas, protegerse con tecnología TEMPEST u ópticas, protegerse con cortinas) desde ubicaciones próximas fuera del perímetro.

Las ramas 3 y 4 se refieren a ataques que explotan al personal de dentro y al acceso físico (local o remoto) respectivamente.

Las ramas 5 y 6 caracterizan los ataques tecnológicos a través de Internet o red telefónica básica ó celular. El considerar los ataques que explotan las debilidades técnicas y no técnicas del funcionamiento de una organización es crítico

Comprometer la supervivencia
Revelación de secretos de la PI de una organización

OR1	Buscar físicamente en la basura papeles y soportes de información descartados por la organización	
	OR1	Inspeccionar las basuras de los papeleras in situ en la organización
	OR2	Inspeccionar dependencias después de su eliminación de la organización
OR2	Monitorizar emanaciones electromagnéticas procedentes de las máquinas de la organización	
	AND1	Estudiar el perímetro físico para determinar la posición de monitorización óptima
	AND2	Adquirir el equipo de monitorización necesario
	AND3	Instalar la monitorización de la organización
	AND4	Monitorizar emanaciones procedentes de la organización
OR3	Recibir ayuda de personal de confianza de dentro de la organización	
	OR1	Plantar espías como personal de dentro de confianza
	OR2	Utilizar el personal de dentro de confianza
OR4	Acceso físico a la red y máquinas informáticas de la organización	
	OR1	Obtener físicamente acceso dentro de la organización a la red Intranet corporativa
	OR2	Obtener acceso físico a máquinas externas
OR5	Atacar a la red corporativa Intranet de la organización utilizando sus conexiones con Internet	
	OR1	Monitorizar las comunicaciones sobre Internet en busca de fugas de información
	OR2	Obtener procesos de confianza para enviar información sensible al atacante utilizando Internet
	OR3	Obtener acceso privilegiado al servidor web
OR6	Atacar a la Intranet de la organización utilizando sus conexiones con la red telefónica pública básica (RTB / RTC / PSTN) o móvil GSM / GPRS	
	OR1	Monitorizar las comunicaciones sobre la red telefónica básica o celular en busca de fugas de información sensible
	OR2	Obtener acceso privilegiado a las máquinas conectadas a la intranet utilizando Internet

Cuadro 2

para hacer más robusta la seguridad y supervivencia.

Los escenarios de intrusión para este árbol de ataque son de nivel muy alto y son:
<1,1>,<1,2>,<2.1, 2.2, 2.3, 2.4>, <3,1>,<3,2>,<4,1>,<4,2>,<5,1>, <5,2>,<5,3>,<6,1>,<6,2>. Un refinamiento del ataque al servidor web (5.3) es el mostrado en el cuadro 3.

Uno de los doce escenarios de intrusión de este subárbol sería:
<1, 2.1, 3.1, 4.1, 5.1>

Ganar acceso privilegiado al servidor web de la organización
AND 1 – Identificar el nombre de dominio de la organización
2 – Identificar la dirección IP del cortafuegos de la organización
OR 1 – Interrogar al servidor de nombres de dominio
2 – Escanear la identificación del cortafuegos
3 – Trazar la ruta a través del cortafuegos al servidor web
3 – Determinar el control de acceso al cortafuegos de la organización
OR 1 – Buscar los puertos de acceso por defecto específicos
2 – Escanear los puertos en busca de cualquier puerto que escuche
4 – Identificar el sistema operativo, versión y tipo del servidor web
OR 1 – Escanear los indicativos de los servicios del sistema operativo para poder identificar el sistema operativo
2 – Sondear la pila TCP/IP en busca de información de características del sistema operativo
5 – Explotar las vulnerabilidades del servidor web de la organización
OR 1 – Acceder directamente a recursos internet compartidos escribibles
2 – Acceder a los datos sensibles desde una cuenta con privilegios en el servidor web

Cuadro 3

Refinamiento de un árbol de ataque. Consistencia del perfil de ataque con la arquitectura de una empresa

Un árbol de ataque puede refinarse a partir de verse comprometido el nodo raíz como una combinación de extensiones manuales y aplicaciones patrón. Las extensiones manuales dependen de la pericia en seguridad de la persona que desarrolla el árbol de ataque. La aplicación patrón también depende del nivel de pericia pero en menor grado. Algo de esta pericia de seguridad se construye en una librería de patrones de ataque. Una buena librería de patrones de ataque proporciona un conjunto de perfiles de ataque que son suficientemente ricos para caracterizar los ataques que pueden tener lugar en un amplio rango de arquitecturas de empresas.

Refinar un árbol de ataque de una empresa concreta implica primero encontrar los perfiles de ataque que son consistentes con la arquitectura de la empresa. El desarrollador busca el patrón de ataque de los perfiles de ataque consistentes para un refinamiento de un camino de ataque contenido en el árbol de ataque de la empresa. Una vez encontrado, el desarrollador puede instanciar y aplicar apropiadamente el patrón de ataque para extender el árbol de ataque de la empresa.

Este proceso de aplicación de patrón entremezclado con la extensión manual continúa hasta que el árbol de ataque se encuentre suficientemente refinado. El modelo de referencia asociado con un perfil de ataque puede verse como una plantilla de arquitectura. Los parámetros de esta plantilla son las variantes del modelo de referencia. Si existe un conjunto de valores para estas variantes que unifica el modelo de referencia del perfil de ataque con alguna porción de la arquitectura de la empresa, se dice que el perfil de ataque es consistente con la arquitectura de la empresa. Los patrones de ataque asociados con el perfil se escriben con respecto al modelo de referencia del perfil y en términos de las variantes del perfil. Estos patrones de ataque son relevantes a la arquitectura de la empresa.

Dos ejemplos de patrones de ataque se representan como indica el cuadro 4.

Patrón de ataque del escaneo de líneas telefónicas
Objetivo: Abrir sesión (ó login) de forma remota con un sistema
Precondición: 1 – El atacante conoce la central telefónica de la organización
2 – El atacante sabe el nombre del usuario
Ataque:
AND 1 – Escanear la central telefónica de la organización para responder a los módem
2 – Determinar que conexión es a través del módem al sistema
3 – Crackear la contraseña de usuario en el sistema
4 – Abrir sesión (login) como usuario en el sistema
Post-condición: El atacante tiene acceso a la cuenta del usuario del sistema

Patrón de ataque de descubrimiento de dirección IP
Objetivo: Identificar la dirección IP del cortafuegos del objetivo
Precondiciones: El atacante conoce el nombre de dominio del objetivo
Ataque:
OR 1 – Interrogar al servidor de nombres de dominio (DNS)
2 – Trazar la ruta a través del cortafuegos al servidor web objetivo
3 – Escanear la dirección IP del cortafuegos
Post-condición: El atacante conoce la dirección IP del cortafuegos objetivo

Cuadro 4

Tareas de una metodología de modelización de ataques

Los modelos de ataques para reconocimiento de escenario se encuentran relacionados con los árboles de ataque utilizados por los ingenieros de seguridad. Sin embargo el propósito de los modelos de ataque no es proporcionar

detalles sobre cómo se realiza cada ataque sino más bien, el énfasis se centra en cómo se detectan y se informa de los atacantes.

Una metodología de modelización de ataques incluye las siguientes tareas:
(a) Identificar los ataques lógicos en un escenario de ataque.- Estos ataques pueden corresponder a sub-objetivos de ataque y cada uno de ellos puede descomponerse hasta que pueda ser detectado por un sensor.
(b) Caracterizar estos ataques lógicos desde el punto de vista de la detección.- Estos ataques pueden detectarse observando ciertos eventos, ciertos estados del sistema o realizando inferencias.
(c) Especificar las relaciones entre estos ataques: En particular existen relaciones temporales (por ejemplo, un ataque sucede antes que otro), relaciones atributo-valor (por ejemplo el objetivo de un ataque es el mismo que la fuente de otro) y relaciones entre pre-requisitos (por ejemplo, un ataque permite que ocurra otro).

Un esquema de modelización de ataques debería poder expresar el conocimiento recopilado en las tareas de modelización descritas anteriormente. Además un esquema de modelización de ataques debería satisfacer los siguientes requisitos para soportar eficientemente el reconocimiento de escenarios de ataque:
1) Extensible para manipular nuevos ataques y sensores.
2) Expresivo para cubrir el intervalo de ataques que se este interesado.
3) No ambiguo para permitir su mecanización.
4) Que permita la reducción de eventos para identificar un evento de seguridad de alto nivel a partir de un gran número de informes de incidente de bajo nivel.
5) Permita implementaciones eficientes.
6) Independiente de la tecnología de los sensores, se supone que los sensores y correlacionadores utilizan medios estándar para comunicarse.

Areas de defensa de los mecanismos de control de riesgo

1) Evitar. Los *riesgos* se pueden puentear si se decide no procesar, o no almacenar o no mantener la información.
2) Transferencia del activo. Los activos en riesgo se pueden trasladan fuera de los límites del área del riesgo, por ejemplo los backup se deben guardar lejos de los CPD (Centro de Proceso de Datos).
3) *Reducción de la amenaza* mediante mecanismos adecuados, por ejemplo, el *cifrado robusto* (por ejemplo AES/3DES/IDEA con claves de 128 bits de longitud o mayores) para las escuchas clandestinas.
4) Reducción de la *vulnerabilidad* mediante mecanismos adecuados.
5) Reducción del *nivel crítico* o de impacto de la misión en base a alterar los procesos para minimizar riesgos.
6) Detección. Análisis de "logs", registros de auditoria, información de los sistemas de detección de intrusiones, etc.
7) Recuperación. Nivel apropiado de procesos y mecanismos de recuperación y backup.

Consideraciones finales

Las alertas de seguridad se producen principalmente por sensores de detección de intrusiones, pero también por otras fuentes como cortafuegos, verificadores de integridad de ficheros, monitores de disponibilidad, etc. Una característica común de estas alertas de seguridad de primer nivel es que cada alerta aislada esta basada en la observación de la actividad que corresponde a una única fase de ataque (explotación atómica, sondeo u otro evento).

El proceso de correlacionar alarmas de diferentes sensores que tienen que ver con diferentes eventos y reconocer escenarios de ataque multi-etapa normalmente es manual y de naturaleza "ad hoc" y por tanto lento y no fiable. Es muy importante automatizar el proceso de reconocimiento de escenarios de ataque, pero existen diversos retos como por ejemplo se necesitan modelizar los escenarios de ataque.

Una vulnerabilidad es una condición en un sistema o en los procedimientos que afecta al funcionamiento del sistema que hace posible realizar una operación que viola la política de seguridad (ó supervivencia) del sistema explícita ó implícitamente.

Una explotación atómica de única fase es aquella que explota una única vulnerabilidad. Una fase de ataque es una explotación atómica de otra actividad realizada por un adversario como parte de una campaña tendente hacia el objetivo del adversario. Un ataque compuesto es un conjunto de una o varias fases de ataques. ❑

Bibliografía

- Areitio, Javier "Identificación, clasificación de Objetivos de Seguridad y Creación de un Modelo de Servicios de Seguridad para las TIC". Revista Española de Electrónica. Noviembre 2003.

- Areitio, Javier "Consideraciones de Seguridad en torno a la Tecnología de Comunicaciones Móviles Celulares GPRS". Revista Española de Electrónica. Mayo 2001.

- McNamara, J. "Secrets of Computer Espionage: Tactics and Countermeasures". John Wiley & Sons Ltd. 2003.

- Horton, M. and Viotto, K. "Hacknotes Network Security Portable Reference". McGraw-Hill. Osborne Media. NY. 2003.

- Fadia, A. "Network Security: A Hacker`s Perspective". Premier Press. 2002.