PLANIFICACIÓN Y EJECUCIÓN DE EVALUACIONES DE SEGURIDAD INFORMÁTICA DESDE UN ENFOQUE DE ETHICAL HACKING

Edgar Vega Briceño

TIC's

3ciencias

PLANIFICACIÓN Y EJECUCIÓN DE EVALUACIONES DE SEGURIDAD INFORMÁTICA DESDE UN ENFOQUE DE ETHICAL HACKING

Edgar Vega Briceño

Editorial Área de Innovación y Desarrollo,S.L.

ÁREA DE INNOVACIÓN Y DESARROLLO, S.L.

C/Alzamora, 17 - 03802 - ALCOY (ALICANTE) info@3ciencias.com

Primera edición: **marzo 2020**

ISBN: **978-84-121459-4-6**

DOI: https://doi.org/10.17993/tics.2020.3

ACERCA DEL AUTOR

El académico Edgar Vega Briceño es Ingeniero en Informática con un posgrado en Administración de la Tecnología de Información y Comunicación por la Universidad Nacional (UNA) de Costa Rica. Es certificado Ethical Hacker por EC-Council y es certificado instructor de la Academia de Cisco en Seguridad de Redes. Ha fortalecido su formación en países como Estados Unidos, India, España y Uruguay. Cuenta con más de 12 años de experiencia como académico en distintas universidades públicas y privadas de Costa Rica. Ha sido consultor en empresa privadas. Actualmente, es académico en la Universidad Nacional (UNA) y sus intereses de investigación se inclinan a la ciberseguridad en sociedades hiperconectadas y la transformación digital para el desarrollo sostenible.

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

CAPÍTULO I: INTRODUCCIÓN

La tecnología ha avanzado tan rápido en los últimos 20 años que los temas de seguridad informática parecen haber pasado desapercibidos. Cualquier debilidad en una aplicación, sensor o infraestructura tecnológica deriva en un riesgo de ciberataque, se convierte en una amenaza que no solo afecta a alguien particular, una institución o una empresa, sino que toda una sociedad estaría en riesgo, es por esto que es necesario conocer los riesgos que se encuentran directamente relacionados con la operación de una organización, sus activos y sus individuos, se debe identificar vulnerabilidades internas y externas y la probabilidad de que ocurra un daño considerable.

Una evaluación de la seguridad informática se puede caracterizar como aquel proceso cuyo fin principal es determinar si el objetivo de la evaluación ya sea éste un host en una red, un sistema de información, una base de datos, una red, un procedimiento, o inclusive un individuo, satisface determinados objetivos de seguridad establecidos previamente o definidos por las buenas prácticas y estándares de la industria (Tejada, 2015).

Tres tipos de métodos de evaluación pueden ser utilizados en este proceso y que se discutirán en el presente documento: verificación, examinación y entrevista. Verificación es el proceso de ejercitar uno o más objetos de evaluación en determinadas condiciones, con el objetivo de comparar comportamiento real con comportamiento esperado. Examinación es el proceso de comprobación, inspección, revisión, observación, estudio y análisis que se le aplica a un objeto de evaluación para facilitar entendimiento, clarificar y obtener evidencia. Entrevista es el proceso de mantener discusiones con individuos o grupos dentro de una organización con objetivos similares al del proceso de examinación, pero con cuestionarios dirigidos y previamente elaborados partiendo de una lista de cumplimiento o mejores prácticas que deberían prevalecer en el ámbito del contexto donde se realizará la evaluación de seguridad.

El objetivo principal de este libro es brindar una guía para desarrollar aspectos de planificación y ejecución necesarios para las evaluaciones de seguridad informática. Aquí se presentan métodos técnicos de verificación y examinación que pueden ser usados por una organización como parte medular de una evaluación de seguridad, incluyendo referencias e indicadores sobre la ejecución de esos métodos que pueden ser de ayuda, por ejemplo, para analistas de seguridad, para entender el impacto que pueden tener sobre los sistemas o redes objetivo de la evaluación.

Para que una evaluación sea exitosa y tenga un impacto positivo en la seguridad de un sistema y por lo tanto en la organización a la que pertenece, la misma debe incluir la realización de actividades adicionales a la verificación y examinación técnica. Este documento también provee guías en esa dirección, presentando una concisa descripción de líneas metodológicas para el desarrollo de una evaluación, que incluyen procedimientos preparativos de la misma, así como la documentación y presentación de los resultados obtenidos durante la evaluación y que deben ser entregados a la organización objetivo.

Se ha propuesto como objetivos de este documento a saber:

- Conocer metodologías y políticas para la evaluación de seguridad informática.
- Planificar una evaluación de seguridad brindando una guía básica sobre cómo determinar qué sistemas evaluar, así como el enfoque a seguir, considerando factores logísticos, definición de plan de trabajo, conformidad legal y con las políticas de la organización.
- Brindar un acercamiento a la ejecución técnica segura y efectiva de la evaluación de seguridad por medio de las técnicas y métodos que se presentan.
- Desarrollar un preciso análisis, diagnóstico, documentación y presentación de los resultados obtenidos, transformando datos técnicos en acciones que le permitan a una organización mitigar riesgos y mejorar la seguridad de sus sistemas.

La estructura que se utilizará en este texto es la siguiente, omitiendo la sección 1 de Introducción:

En la sección 2 se muestra una descripción de aspectos básicos involucrados en un análisis y evaluación de seguridad informática. En la sección 3, se introducen los lineamientos metodológicos esenciales a seguir en la conducción de un proceso de evaluación de seguridad, identificando las tres actividades principales: preparación y planificación, ejecución de tareas y documentación y la presentación de resultados. Estas tres actividades marco son desarrolladas en detalle en las secciones 4 y 5 respectivamente.

Por último, se indicarán una serie de conclusiones que reafirman la importancia de realizar una evaluación de seguridad informática bajo un proceso planificado y estructurado que permita obtener resultados idóneos para la toma de decisiones.

CAPÍTULO II: EVALUACIÓN DE SEGURIDAD INFORMÁTICA

Dado que el avance hacia una sociedad más digitalizada e hiperconectada en donde las empresas cada vez hacen un uso más exhaustivo de las Tecnologías de Información y Comunicación se hace necesario evaluar la seguridad de los sistemas de información de forma integral como parte de una cultura organizacional. Solarte (2015) y otros autores afirman que:

> *Actualmente los sistemas de información, los datos contenidos en ellas y la información son los activos más valiosos para las organizaciones empresariales y se hace necesario brindarles una protección adecuada frente a las posibles intrusiones derivadas de las vulnerabilidades existentes en sus sistemas de seguridad. Una manera efectiva de descubrir estas vulnerabilidades y amenazas existentes es iniciando los procesos diagnósticos que permitan establecer el estado actual de la seguridad dentro de la organización, teniendo en cuenta la normatividad vigente y los procesos de análisis y evaluación de riesgos (p. 493).*

Existe una gran variedad de técnicas de verificación y examinación para evaluar la seguridad de sistemas y redes. Se discute a continuación tres de ellas que serán desarrolladas en las próximas secciones. Según Baloch (2017):

> *Técnicas de revisión: estas son técnicas de examinación usadas para evaluar sistemas, aplicaciones, redes, políticas y procedimientos con el objetivo de descubrir vulnerabilidades. Las mismas son usualmente realizadas en forma manual e incluyen: revisión de documentación, bitácoras y reglas, revisión de configuración de sistemas, "sniffing" de redes y revisión de integridad de archivos.*
>
> *Técnicas de identificación: estas técnicas permiten identificar sistemas, puertos, servicios y potenciales vulnerabilidades presentes en los mismos. Las técnicas pueden ser ejecutadas manualmente, pero generalmente se usan herramientas automáticas. Las mismas permiten realizar descubrimiento de redes, identificación de puertos y servicios, escaneo de vulnerabilidades sobre los mismos y examinación de seguridad de aplicaciones.*
>
> *Técnicas de validación de vulnerabilidad: estas técnicas permiten corroborar la presencia de vulnerabilidades conocidas y pueden también ser ejecutadas en forma manual o con la asistencia de herramientas, dependiendo de las*

técnicas y habilidades del equipo de evaluación. Este tipo de técnicas incluye: descifrar contraseñas, pruebas de intrusión, ingeniería social y pruebas de seguridad de aplicaciones.

Dado que ninguna de las técnicas enumeradas anteriormente puede proporcionar una visión completa de la seguridad de una red o sistema, en general las organizaciones deben realizar una combinación de algunas de las mismas para poder desarrollar una evaluación de seguridad confiable y robusta. Por ejemplo, la realización de una prueba de penetración en el caso general se basa primero en efectuar la identificación y escaneo de vulnerabilidades de los puertos y servicios de una red, para detectar hosts y servicios que luego pueden ser objetivo de una acción de penetración. En esta sección, el foco estará situado en explicar cómo las diferentes técnicas pueden ser utilizadas, sin especificar qué técnicas deben ser usadas en qué circunstancias. En la sección 4, se describe una metodología de análisis de seguridad, que involucra fases de trabajo claramente diferenciadas y se verá en secciones posteriores qué técnica y herramienta puede/debe ser usada en cada fase.

CAPÍTULO III: TÉCNICAS DE EVALUACIÓN

3.1. Evaluación externa (caja negra) y evaluación interna (caja blanca)

Una evaluación puede ser conducida desde fuera del perímetro de seguridad de la organización. Esto ofrece la posibilidad de entender cómo el sistema de seguridad de la organización puede ser percibida por una visión externa a la misma, por ejemplo, cómo se ve desde la Internet. El objetivo principal es identificar vulnerabilidades que podrían ser explotadas por un atacante externo a la organización. Bajo este esquema, el experto que realiza la evaluación no tiene información alguna de la infraestructura y sistemas objetivos y se le conoce como análisis de caja negra (Bracho *et al*., 2017).

Una evaluación externa de la seguridad de una organización generalmente comienza ejecutando técnicas de reconocimiento para la obtención de datos de registro que son públicos. Luego, se enumeran los hosts y servicios usando técnicas de descubrimiento y escaneo de red. Dado que defensas perimetrales, como muros de fuego, enrutadores y listas de control de acceso, usualmente limitan los tipos de tráfico permitido desde y hacia la red, el analista de seguridad usualmente utiliza técnicas que permiten evitar, o vulnerar esas defensas, de la misma forma en que haría un atacante. La evaluación de seguridad externa, también generalmente se concentra en descubrir vulnerabilidades de métodos de acceso, tales como puntos de acceso inalámbrico, módems y portales a servidores internos.

Por otro lado, para la realización de una evaluación interna de seguridad, el analista desarrolla su trabajo desde la red interna de la organización, ya sea asumiendo la identidad de un usuario confiable o actuando como un atacante que ha vulnerado las defensas del perímetro, bajo este esquema hay acuerdos previos con la organización y una planificación para la realización de este análisis. Este tipo de evaluaciones permiten ilustrar el tipo de vulnerabilidades que podrían ser explotadas desde el interior de la organización y el impacto que causa sobre la misma. Una evaluación interna de seguridad también se focaliza en la seguridad a nivel de sistemas y configuración, incluyendo configuración de aplicaciones y servicios, autenticación, control de acceso y “hardening” de sistemas de información.

Los analistas que desarrollan este tipo de evaluación son provistos de un cierto nivel de privilegio de acceso a los sistemas, generalmente como usuarios generales, y luego, dependiendo del objetivo de la evaluación, intentan acceder a mayores niveles de privilegios, por ejemplo, obteniendo privilegios de administrador para

ganar acceso adicional a los sistemas y la red. Este tipo de análisis de seguridad es conocido como evaluación de caja blanca.

La noción de caja negra o caja blanca se origina en el contexto de la disciplina de prueba y evaluación de software, donde en el primer enfoque la verificación de conformidad del código implementado con los requerimientos del sistema se efectúa sin disponer del código mismo. En el contexto de las evaluaciones de seguridad informática, el desarrollo de una evaluación de seguridad en modo caja negra refiere al uso de técnicas y métodos para la identificación de vulnerabilidades sin tener conocimiento del sistema. Por ejemplo, el objetivo de una prueba de penetración en modo caja negra es simular la realización de un ataque al sistema en idénticas condiciones a las de un posible atacante externo.

Una evaluación en modo caja blanca refiere al uso de una metodología donde el profesional de seguridad tiene un conocimiento detallado del objetivo de seguridad, ya sea este una red, un sistema o una aplicación. El objetivo, por ejemplo, de una prueba de penetración desarrollado en modo caja blanca es básicamente el de simular el modus operandi de un actor malicioso interno a la organización (o un atacante que logró una intrusión a la seguridad perimetral y posiblemente realizó una escala de privilegios horizontal o vertical) quien puede tener algún conocimiento del funcionamiento y/o credenciales de acceso al objetivo de evaluación.

¿Existe alguna combinación de ambas? Si, y se conoce como un análisis de caja gris que combina ambos análisis antes expuestos y refiere al uso de una metodología donde el analista de seguridad es provisto con algún tipo de credenciales (un usuario/contraseña de una red o de una aplicación, con mínimos privilegios, por ejemplo) pero sin contar con conocimiento acabado del entorno, arquitectura, topologías, aplicaciones del objetivo de evaluación. Este análisis persigue los mismos objetivos que uno de caja negra, pero tratando de utilizar una menor cantidad de tiempo.

Es importante mencionar que en el caso que la organización desee efectuar tanto una evaluación externa como una interna, la externa es la que usualmente se ejecuta en primer lugar. Esto es sobre todo útil cuando son los mismos analistas los que realizan ambas evaluaciones. De esta forma, la evaluación externa se realiza sin contar con la información adicional que provee tener acceso a la red y sistemas, y, por lo tanto, igualando las condiciones con un atacante externo.

3.2. Evaluación abierta y encubierta

En un análisis de seguridad abierto, también conocido como pruebas de sombrero blanco, la evaluación de seguridad ya sea externa y/o interna, es realizada bajo el conocimiento y con el consentimiento de la organización y posiblemente del staff de TI de esta.

Esto implica algunas ventajas:

Al estar en conocimiento de la realización de la evaluación, el staff de TI puede colaborar en proveer guías para reducir el impacto de la evaluación.

La evaluación puede ser beneficiosa como entrenamiento para el equipo, al observar las actividades y los métodos usados por los analistas para evaluar y potencialmente vulnerar las medidas de seguridad implantadas.

En un análisis de seguridad encubierto, también conocido como pruebas de sombrero negro, el analista se sitúa en posición de atacante o actor malicioso desarrollando su actividad sin el conocimiento del staff de Tecnologías de Información (TI), pero con el conocimiento y permiso de la dirección de la organización. Este tipo de evaluación es muy útil para evaluar los controles técnicos de seguridad, respuesta del staff de TI ante la ocurrencia de incidentes de seguridad, así como el conocimiento del staff y su implantación de las políticas de seguridad de la organización. El propósito principal de este tipo de evaluación es poder examinar el daño o impacto que un atacante podría causar, sin importar la identificación de vulnerabilidades de los sistemas.

3.3. Técnicas de revisión

Estas técnicas se caracterizan por examinar en forma pasiva sistemas, aplicaciones, redes y procedimientos con el objetivo de identificar vulnerabilidades. Asimismo, con estás técnicas se recoge información que permite facilitar y optimizar otras técnicas de evaluación. A continuación, se describen brevemente algunas de las técnicas de revisión más comunes.

3.3.1. Revisión de políticas, procedimientos y documentación

El objetivo es determinar si los aspectos técnicos involucrados por las políticas y procedimientos de seguridad de la organización están actualizados y tienen un adecuado alcance. Estos documentos son en general desatendidos durante la realización de una evaluación técnica.

Los documentos que deben ser revisados para determinar su exactitud y completitud técnica, incluyen: políticas, arquitecturas y requerimientos de seguridad, procedimientos operativos estándar, planes de seguridad de los sistemas y acuerdos de autenticación, de entendimiento y para la interconexión de sistemas, así como planes de respuesta a incidentes de seguridad.

Los resultados de la revisión de documentos pueden ser utilizados para refinar otras técnicas de evaluación y examinación. Por ejemplo, si una política de gestión de contraseñas tiene requerimientos específicos en lo que refiere al largo y complejidad de estas, esta información puede a su vez ser utilizada para configurar herramientas de "password-cracking" para mejorar la eficiencia de su ejecución.

3.3.2. Revisión de bitácoras

La revisión de bitácoras o logs de sistemas permite determinar si los controles de seguridad establecidos e implantados están registrando la información adecuada y si la organización está respetando las políticas de gestión de registros.

Ejemplos de información registrada que podría ser útil cuando se realiza una evaluación de seguridad es listada a continuación:

- Bitácoras del servidor de autenticación o logs de sistema que incluyan los intentos, tanto exitosos como fallidos, de autenticación.
- Bitácoras generadas por los IDS (Sistemas de Detección de Intrusiones, por sus siglas en inglés) y/o IPS (Sistemas de Prevención de Intrusiones, por sus siglas en inglés), que pueden incluir actividad maliciosa y uso inapropiado de los recursos.
- Bitácoras de muros de fuego y enrutadores, los que pueden incluir conexiones que indiquen que un dispositivo interno ha sido comprometido (por ejemplo, software malicioso, puertas traseras, etc.).
- Bitácoras de aplicación, que pueden incluir intentos no autorizados de conexión, cambios de cuentas, uso de privilegios e información de uso de las aplicaciones y las bases de datos.
- Logs de antivirus, que pueden incluir fallas de actualización u otras indicaciones de desactualización de firmas y software.
- Bitácoras de seguridad, en particular de gestión de parches y registros de algunos IDS/IPS, que pueden incluir información sobre vulnerabilidades conocidas de servicios y aplicaciones.

Efectuar la revisión de bitácoras en forma manual puede ser extremadamente complejo e ineficaz. Existen herramientas tanto privadas como libres que automatizan procedimientos de auditoría y que permiten reducir el tiempo de revisión y de generación de reportes.

3.3.3. Revisión de la configuración

Este es el proceso mediante el que se identifican debilidades en los controles de configuraciones de seguridad, tales como que los sistemas no han sido configurados como lo requieren las políticas de seguridad. Por ejemplo, este tipo de revisión permitirá revelar si existen activos servicios y/o aplicaciones en forma innecesaria, configuraciones inapropiadas de cuentas y contraseñas de usuario, políticas de autenticación y respaldos.

Los analistas que realizan estas revisiones se apoyan en guías de configuración de seguridad y listas de verificación que el sistema ha sido configurado para minimizar los riesgos de ocurrencia de incidentes de seguridad. En general, es preferible que estos chequeos sean asistidos por cierto nivel de automatización, ya que dedicar a una persona a chequear cientos o miles de ítems en forma manual no sólo es tedioso sino también propenso a que se cometan errores.

3.3.4. Análisis de la red (network sniffing)

Esta es una técnica pasiva, que consiste en monitorear las comunicaciones en la red, decodificando protocolos y examinando información de encabezados y carga útil (payload), registrando información de interés. Esta es también una técnica que puede ser usada para la identificación y análisis de un objetivo de seguridad (Vieites, 2011).

Esta técnica permite:

- Capturar y replicar tráfico de red.
- Efectuar descubrimiento pasivo de red (por ejemplo, identificar los dispositivos activos en la red).
- Identificar actividades no autorizadas e inapropiadas, como la transmisión no encriptada de información sensible.
- Recolectar información, como nombres de usuario y contraseñas no encriptadas.

Esta técnica casi no tiene impacto en sistemas y redes, siendo el más notable el que genera sobre la utilización del ancho de banda y de los recursos de computación. Una organización pude implantar un proceso de análisis de red en diferentes puntos del ambiente, por ejemplo:

- En el perímetro, para validar el tráfico entrante y saliente de la red.
- Detrás de los muros de fuego, para validar que las reglas efectivamente filtran el tráfico.
- Detrás de sensores de detección o prevención de intrusos, para determinar si las firmas se están gestionando adecuadamente.
- En un segmento específico de la red, por ejemplo, para validar protocolos de cifrado.

Es importante mencionar una limitación de esta técnica, y es que si el tráfico está encriptado el analista podrá observar que una comunicación se está realizando, pero no podrá visualizar el contenido. Otra limitación importante es que el alcance de acción de esta técnica es el segmento de red sobre el que está instalado.

3.3.5. Revisión de la integridad de archivos (checksum)

Esta técnica provee una forma de identificar que un sistema de archivos ha sido modificado (en forma autorizada o no) calculando y registrando una suma de chequeo para cada archivo que se desee monitorear. Estas sumas de verificación son luego recalculadas y comparadas con los valores registrados, lo que permite identificar potenciales modificaciones de los archivos. Aunque una herramienta de revisión de integridad no requiere un alto factor de intervención humana, el mismo debe ser usado muy cuidadosamente. Esta técnica es realmente efectiva cuando los sistemas de archivos, o más precisamente sus correspondientes sumas de verificación, son comparados con una base de datos referencia que ha sido creada y es mantenida en forma segura. Para la generación de tokens de integridad es recomendable usar sumas de verificación criptográficos como, por ejemplo, Secure Hash Algorithm 2 (SHA-2).

3.4. Identificación de objetivos de evaluación

En esta sección se describen técnicas para identificar objetos a evaluar. Las mismas se focalizan en identificar dispositivos activos en la red, así como los puertos y servicios asociados y analizar potenciales vulnerabilidades de estos. El analista de seguridad hará uso de esta información para profundizar su exploración y eventualmente

validar la existencia de vulnerabilidades. Las organizaciones a menudo usan también técnicas que no involucran tecnología para identificar activos que deben ser analizados. Por ejemplo, las organizaciones suelen contar con un inventario que lista los activos que pueden ser instancias de evaluación. Otro ejemplo sería un analista que efectúa una recorrida por las instalaciones de la organización tratando de identificar activos que no fueron detectados por medios tecnológicos, como hosts que estaban bajos o desconectados de la red cuando se estaban usando las herramientas de identificación.

En esta sección del documento se hace énfasis en brindar una breve descripción de las técnicas y a posicionar sus características más relevantes, más adelante se entrará en detalles.

3.4.1. Descubrimiento de la red

Esta técnica consiste en la utilización de diversos métodos para descubrir hosts activos en una red, identificar debilidades y adquirir un adecuado entendimiento de la operativa de una red. Se pueden usar técnicas tanto pasivas como activas para el descubrimiento de dispositivos en la red. Las técnicas pasivas utilizan principalmente un analizador de protocolos para monitorear tráfico y registrar las direcciones IP de los hosts activos y pueden asimismo reportar qué puertos están en uso y qué sistemas operativos han sido detectados en la red. Las técnicas activas envían, generalmente usando una herramienta automatizada, distintos tipos de paquetes de red, como ICMP pings, para solicitar respuestas desde hosts de la red. Una de estas actividades, conocida como firma del sistema operativo, le permite a un analista (o un atacante) determinar los sistemas operativos presentes en la red enviándole una combinación de tráfico de red normal, anormal o aún ilegal.

Las ventajas de descubrimiento activo, en comparación con el pasivo, es que una evaluación puede ser realizada desde una red diferente a la red objetivo y usualmente requiere menos tiempo para recolectar información relevante. El descubrimiento pasivo, para asegurar que todos los hosts son identificados, requiere la existencia de tráfico que cubra todos los puntos, lo que insume, especialmente en grandes empresas, de una gran cantidad de tiempo.

La desventaja de las técnicas activas es que tienden a generar “ruido” en la red, lo que a veces puede afectar el rendimiento de esta. Dado que estas técnicas envían consultas masivas, con el objetivo de recibir respuestas, esta actividad adicional en la red puede enlentecer el tráfico o causar la pérdida de paquetes en redes no configuradas adecuadamente, sobre todo si el tráfico es de alto volumen. Las

técnicas activas pueden, asimismo, provocar alertas sistema de detección de intrusos y provocar que descubran el escaneo que se está realizando a la red.

Por otro lado, tanto en el caso de técnicas activas como pasivas, la información recibida es generalmente incompleta. Por ejemplo, solamente los hosts que están conectados y operativos durante la tarea de descubrimiento serán identificados. Aunque las técnicas pasivas solamente detectarán dispositivos que transmiten o reciben comunicaciones durante el período de descubrimiento, existe software de gestión de redes que puede proveer capacidades continuas de descubrimiento y generar alarmas cuando un nuevo dispositivo está presente en la red. Asimismo, muchas herramientas de descubrimiento pueden configurarse para ser ejecutadas regularmente. Esto provee resultados más confiables y completos que si se corren estas herramientas en forma esporádica.

3.4.2. Identificación de puertos y servicios

Estas técnicas consisten en utilizar herramientas para identificar puertos y servicios, como FTP o HTTP, operando en equipos activos, así como la aplicación que está ejecutando cada servicio identificado, tales como Microsoft Internet Information Server (IIS) o Apache para el servicio HTTP en el caso de servidores GNU/Linux. Las organizaciones deben aplicar este tipo de técnicas para identificar hosts si esto ya no ha sido realizado de otra forma (por ejemplo, por descubrimiento de red) y así registrar servicios potencialmente vulnerables. Esta información puede usarse, por ejemplo, para determinar objetivos de una evaluación de seguridad realizando una prueba de penetración. La gran mayoría de herramientas básicas pueden identificar hosts y puertos abiertos, pero hay algunos de ellos que pueden proveer información adicional, que, por ejemplo, puede ser usada en el proceso de identificación de sistemas operativos conocido como firmas de sistemas operativos.

Algunas herramientas pueden ayudar a identificar la aplicación que se está ejecutando en un puerto a través de un proceso llamado identificación de servicios, NMAP es un ejemplo clásico y que más adelante será mencionado. Por otro lado, aunque la realización de escaneo de puertos permite identificar hosts activos, sistemas operativos, puertos, servicios y aplicaciones, esta actividad no permite identificar vulnerabilidades. Se debe realizar una investigación adicional para confirmar la presencia de protocolos inseguros, programa malicioso, aplicaciones no autorizadas y servicios vulnerables. Para identificar servicios vulnerables, por ejemplo, al analista compara los números identificados de versión de los servicios con una

lista de versiones vulnerables o directamente efectúa un escaneo automatizado de vulnerabilidades como será discutido en la próxima sección.

3.4.3. Escaneo de vulnerabilidades

Al igual que en el caso de identificación de puertos y servicios, el escaneo de vulnerabilidades identifica hosts y sus atributos (como sistemas operativos, aplicaciones, puertos abiertos) pero además intenta identificar vulnerabilidades complementando así los resultados provenientes de un análisis realizado por un analista a partir de los resultados de escaneo. Muchas herramientas de análisis de vulnerabilidades están equipadas para aceptar resultados generados por procesos de descubrimiento de red y de identificación de puertos y servicios.

Estas técnicas pueden ayudar a detectar versiones desactualizadas de software, ausencia de parches y problemas de configuración, así como validar la conformidad con las políticas de seguridad de la organización. Las mismas permiten:

- Chequear conformidad con uso de aplicaciones y políticas de seguridad.
- Proveer información sobre objetivos de una prueba de penetración.
- Proveer información sobre cómo mitigar vulnerabilidades detectadas.

Un escaneo de este tipo puede ser realizado contra un host, ya sea localmente o desde la red. En el caso de escaneo local, el escáner es instalado en el host. Esto se hace principalmente para identificar configuraciones incorrectas y/o vulnerabilidades del Sistema Operativo, así como de aplicaciones instaladas que podrían ser explotables tanto en forma local como desde la red.

3.4.4. Escaneo en redes inalámbricas

Las tecnologías inalámbricas posibilitan que uno o más dispositivos puedan comunicarse sin necesidad de contar con conexiones físicas, tales como redes o cables periféricos. Estas abarcan desde simples tecnologías, como teclados y ratones inalámbricos, hasta redes complejas de teléfonos celulares y redes locales inalámbricas empresariales (WLAN). A medida que se incrementa el número y disponibilidad de dispositivos inalámbricos en una organización, es importante que ésta implemente evaluaciones y aseguramiento de los ambientes inalámbricos. La realización de escaneos inalámbricos puede ayudar a las organizaciones a determinar acciones correctivas necesarias para mitigar los riesgos que presentan las tecnologías inalámbricas. Al planear una evaluación técnica de la seguridad inalámbrica, es importante tomar en cuenta las siguientes consideraciones:

- La posición física del dispositivo escaneado, ya que la proximidad de un edificio a un área pública o su localidad en un área metropolitana puede incrementar el riesgo de amenazas inalámbricas.
- La seguridad de los datos que serán transmitidos usando tecnologías inalámbricas.
- Qué tan frecuente los dispositivos inalámbricos se conectan y desconectan del ambiente, así como el nivel típico de tráfico de estos dispositivos (por ejemplo, determinando si la actividad es ocasional o razonablemente constante). Esto es importante ya que solamente dispositivos activos pueden ser detectados durante un escaneo de este tipo.
- La presencia de sistemas de detección/prevención de intrusos en redes inalámbricas (WIDPS, por sus siglas en inglés) que ya puedan permitir recolectar la información que sería colectada por medio de la evaluación.

Un escaneo inalámbrico debería ser realizado usando un dispositivo móvil equipado con software de análisis inalámbrico. La herramienta o software de escaneo debería permitir configurar al dispositivo para efectuar escaneos específicos y para hacerlo tanto en modo activo como pasivo. Este software debería poder ser configurable a sí mismo, para poder identificar desviaciones de los requerimientos de configuración de seguridad inalámbrica de la organización.

3.5. Validación de vulnerabilidades

Esta sección está dedicada a la presentación de técnicas de validación de vulnerabilidades, estás técnicas normalmente utilizan la información generada por la aplicación de técnicas de identificación y análisis para profundizar en la exploración de la existencia de potenciales vulnerabilidades. El objetivo es probar que existe una vulnerabilidad y demostrar el tipo de exposición a la que se puede ver enfrentada la organización en caso de que la misma sea explotada. La aplicación de este tipo de técnicas en el transcurso de una evaluación de seguridad puede involucrar riesgos por el tipo de impacto que puede acusar la utilización de estas sobre los sistemas y/o redes objetivo (Polanía, 2016).

3.3.1. Descifrado de contraseñas

Cuando un usuario de un sistema ingresa una clave, un resumen del cifrado, comúnmente conocido como hash, es generado y comparado con el hash registrado en el sistema de gestión de contraseñas. Si los hashes coinciden, el usuario (o aquel que clama ser el usuario) es autenticado. El descifrado de contraseñas es el

proceso mediante el cual se intenta recuperar contraseñas a partir de los hashes de contraseñas, ya sea que estén estos salvados en memoria persistente del sistema o que hayan sido enviados en la red.

Un método muy utilizado para la generación de hashes es lo que se denomina un ataque de diccionario, el que usa para generar los hashes todas las palabras de un diccionario o un archivo de texto. Otro método para implementar descifrado de contraseñas es el llamado ataque de fuerza bruta. Este tipo de ataques consiste en generar todas las posibles contraseñas (y sus hashes) de un cierto tamaño y basado en un determinado conjunto de caracteres (por ejemplo, los definidos por la política de contraseñas de la organización). Dado que la entropía de posibles contraseñas puede ser muy grande, este proceso puede ser muy costoso en tiempo, sin embargo, es muy probable que tarde menos que el intervalo de tiempo que definen las políticas para el cambio de contraseñas. Teóricamente, dado suficiente tiempo y poder de procesamiento, todas las contraseñas pueden ser quebradas por un ataque de fuerza bruta. Analistas y atacantes a menudo usan varias máquinas para calcular en paralelo el algoritmo de craqueo, reduciendo así drásticamente los tiempos de ejecución, sobre todo hoy en día que se cuenta con tanto poder de cómputo de fácil aprovisionamiento en la nube. Finalmente, este proceso se puede efectuar usando lo que son conocidas como tablas arcoíris (*rainbow tables*), que son tablas con hashes pre-calculados. Por ejemplo, una tabla de éstas podría ser la que contiene todos los hashes de todas las contraseñas que se pueden formar a partir de un cierto conjunto de caracteres y de cierto largo. Esta técnica tiene ciertas desventajas: la generación de las tablas generalmente requiere mucho tiempo y su almacenamiento mucho espacio, pero, sobre todo, pueden ser inefectivas cuando se utiliza salt1 para la generación de hashes. Los programas descifradores de contraseñas son usualmente ejecutados durante el desarrollo de una evaluación de seguridad para validar y asegurar conformidad con las políticas de contraseñas de la organización objeto del análisis. Si este proceso es ejecutado off-line tiene muy poco impacto sobre la red o el sistema y los beneficios que genera son realmente relevantes.

3.3.2. Prueba de intrusión

Una prueba de intrusión es básicamente una prueba de seguridad en el que los analistas replican la actividad propia de un atacante para poder identificar formas y métodos que le permitan vulnerar la seguridad de una aplicación, un sistema o una red. Generalmente, este tipo de actividad involucra efectuar ataques reales sobre

1 Comprende bits aleatorios que se usan como una de las entradas en una función derivadora de claves.

sistemas y datos usando las herramientas y técnicas que son comúnmente utilizadas por atacantes reales. Una prueba de intrusión generalmente involucra también la utilización de métodos no técnicos. Por ejemplo, un evaluador puede vulnerar procedimientos y controles para la seguridad física, para poder conectarse a una red, robar equipamiento, capturar información sensible o interrumpir las comunicaciones. Otra herramienta, no-técnica, para la realización de ataques es el uso de ingeniería social, tal como suplantar a un agente de la mesa de servicio de ayuda y llamar a un usuario para requerirle su contraseña, o en el caso inverso, llamar a la mesa de ayuda reemplazando a un usuario requiriendo el cambio de contraseña. Las técnicas de las pruebas de penetración serán discutidas en mayor detalle más adelante (Pinzón, Talero, y Bohada, 2017).

3.3.3. Ingeniería Social

La realización de un acto de ingeniería social consiste en intentar engañar a una persona para que revele información sensible, una contraseña, por ejemplo, que pueda ser usado para atacar sistemas o una red. Es generalmente una técnica usada para testear el "factor humano" de la seguridad y puede revelar debilidades, tales como el no seguimiento de procedimientos por parte de usuarios de los sistemas o redes. La ingeniería social puede ser aplicada a través del uso de medios diversos, incluyendo análogos (conversaciones por teléfono o en persona) y digital (e-mail o mensajería instantánea). Una de las formas de ingeniería social digital es conocida con el nombre de Phishing, donde el atacante intenta apoderarse de información como números de tarjetas de crédito, número de la seguridad social, identificadores de usuarios y contraseñas (Jagatic *et al*., 2007).

CAPÍTULO IV: METODOLOGÍA PARA EVALUACIONES DE SEGURIDAD

En toda actividad, cuando se desea mantener un enfoque que permita analizar un problema de una forma sistemática y con cierta disciplina, es imperioso contar con un conjunto de métodos a seguir. Cuando se hace referencia a un proceso de evaluación de seguridad es necesario realizar una selección de procedimientos concretos que permitan, entre otros, identificar los objetivos, garantizar la coherencia y la estructura de la evaluación, minimizar los riesgos y comunicar adecuadamente los resultados. Varias organizaciones describen metodologías para diferentes tipos de evaluaciones de seguridad, como por ejemplo el Instituto para la Seguridad y Metodologías Abiertas (ISECOM, por sus siglas en inglés) propone el Open Source Security Testing Methodology Manual (OSSTMM). El OSSTMM incluye lineamientos de acción, conjuntos de pruebas, plantillas de referencia y según los autores: "El objetivo de este manual es crear un método aceptado para ejecutar una prueba de seguridad minuciosa y cabal" (Herzog, 2003).

Otra referencia relevante es el Open Information Systems Security Group (OISSG) que propone el marco de trabajo: System Security Assessment Framework (ISSAF), en donde también describen un conjunto de lineamientos y acciones a seguir (Hallberg, Hunstad, y Peterson, 2005).

Por otro lado, Technical Guide to Information Security Testing and Assessment (NIST), no aconseja ninguna metodología sobre otras. En su lugar, proporciona lineamientos con el fin de asistir en la toma de decisiones al momento de adoptar una metodología existente o combinar varias según las necesidades.

Tomando como referencia las metodologías antes mencionadas, se puede decir que, en el nivel más abstracto, la metodología a utilizar tiene que contemplar aspectos que hagan referencia a los siguientes puntos:

- *Planificación y preparación:* esta fase es de suma importancia en toda evaluación de seguridad que se lleve a cabo, comprende pasos como entrevistas o reuniones de trabajo en las cuales se establecen las metas, objetivos y propósitos; se fijan las expectativas y se presenta al equipo de trabajo. Como en todo proyecto, se establece la relación contractual entre las partes y se fija un plan de gestión, el cual incluye: el alcance, los cronogramas, las responsabilidades y las limitaciones que puedan existir. Se establecen los horarios de trabajo y las pruebas de campo a utilizar según los objetivos establecidos.

- *Ejecución de tareas:* en esta etapa se realizan las pruebas de campo propiamente dichas, la finalidad principal es descubrir las problemáticas de seguridad asociadas a los objetivos, como ser: vulnerabilidades, accesos a información privilegiada y/o privada, entre otros. En general se adopta un enfoque basado en capas, comenzando por el reconocimiento, seguido de la identificación y descubrimiento, para luego de recopilada la información necesaria realizar el análisis, y si corresponde, explotar (atacar) las problemáticas identificadas. Esto último se podría suponer como otro alcance para otro proyecto, pues se deben valorar otros factores de interés para la organización objetivo. Es importante mencionar, que las actividades de esta fase, si bien seguirán el enfoque basado en capas, serán específicas para cada objetivo establecido en la etapa de planificación. Al término de esta fase, los analistas de seguridad habrán identificado las brechas de seguridad de los objetivos, en cuyo caso deberán reportarla a los interesados de una forma clara y concisa. De todas maneras, hay que tener en cuenta que los problemas detectados no son necesariamente todos los existentes. Que no se detecten problemas no quiere decir que no existan, simplemente puede darse la situación en la que el tiempo dedicado y las capacidades de los evaluadores no fueron suficientes para su detección. Hay que tener en cuenta que llegar al término de esta fase sin problemas detectados, no es necesariamente un mal resultado, quiere decir que el objetivo se encuentra seguro frente a agentes maliciosos que cuenten con una experiencia y tiempo similar a los analistas de seguridad involucrados. Es aquí donde cobra gran importancia la fase de planificación, junto a la experiencia del equipo de trabajo y las expectativas fijadas.
- *Documentación y presentación:* Una vez concluida la fase anterior, luego de finalizadas las pruebas, analizados los resultados y descartados los falsos positivos, es necesario comunicar los resultados. Para ello, es pertinente escribir un informe detallado de las pruebas, indicando los resultados, las recomendaciones y posibles acciones a llevar adelante para subsanar los problemas. Para la escritura de dicho informe hay que tener en cuenta el público objetivo. En general, se incluyen secciones que van dirigidas a todo tipo de público y otras con un enfoque más profundo dirigido a técnicos. También es una buena práctica incluir algún tipo de evidencia gráfica como: captura de pantallas, videos, fotografías, entre otros. Dicho tipo de material ayuda a comprender y tomar conciencia de los problemas a los cuales se puede estar expuesto. En las siguientes secciones se procede a describir en más detalle cada una de las fases aquí descritas, poniendo especial foco en la fase de ejecución de tareas.

CAPÍTULO V: FASES PARA LA EVALUACIÓN DE SEGURIDAD

5.1. Planificación y preparación

Como se mencionó anteriormente esta fase es de suma importancia en toda evaluación de seguridad, de ella depende gran parte del éxito que pueda tener una tal evaluación de este tipo en una determinada organización. En esta sección se presentan los puntos para tener en cuenta al momento de planificar y preparar un análisis de seguridad.

5.1.1. Entrevistas previas

Para planificar una evaluación de seguridad lo ideal es realizar una reunión inicial entre representantes de la organización que recibirá el servicio y algún representante del equipo de seguridad que lo llevará a cabo. En dicha reunión se examinarán las cuestiones relativas al alcance y objetivo del análisis, así como se definirán las contrapartes involucradas. Esta reunión permitirá a los analistas de seguridad elaborar una propuesta y, en caso de que corresponda, un presupuesto adecuado para la organización.

5.1.2. Definición de objetivos

Los objetivos y alcance de una evaluación de seguridad deben ser claros, una organización que solicita un análisis sin razones y/o propósitos específicos no debería sorprenderse si los resultados que obtiene son genéricos o sin valor. A partir de esta instancia los analistas de seguridad deben comenzar a asesorar a la organización, explicando las metodologías a utilizar, los posibles objetivos y el alcance de las tareas.

El alcance de las tareas debe estar claramente especificado como parte del acuerdo entre los analistas de seguridad y la organización. Siempre que sea posible se deben evitar los alcances ambiguos y los objetivos desmedidos. Cuando la extensión del trabajo se encuentra bien delimitada y acorde a las necesidades de la organización, el trabajo de evaluación de seguridad se realizará con mayor precisión y los resultados serán más fiables. Si el analista infiere que hay una gran cantidad de objetivos a ser analizados, se deben dividir las tareas en unidades pequeñas, definiendo metas específicas para cada uno de estos objetivos.

Es muy importante hacer algunas preguntas generadoras y que un analista de seguridad tendría que hacer en la organización. Por ejemplo, ¿qué se quiere evaluar

específicamente (el propósito)? y ¿cuál es la razón o la motivación para solicitar los servicios de un experto en seguridad informática?

Las respuestas a las preguntas anteriores suelen ser variadas, y es frecuente que las motivaciones/razones sean de origen diverso. A menudo las organizaciones se ven comprometidas por un ataque (acción reactiva) y acuden a expertos de seguridad para que evalúen la situación y se puedan cuantificar las pérdidas o evaluar los daños. Otras veces, se encuentran presionadas por terceros, no es descabellado que una organización al establecer una relación de negocios con otra exija como parte del contrato que se le realice una auditoría de seguridad a su futuro socio o que haya presiones de clientes también. Más allá de las motivaciones, es importante establecer con la organización el propósito del análisis, es decir, cuál es el fin u objetivo que se persigue.

Entre los diferentes propósitos se encuentra la decisión de si el personal de la organización debe ser informado antes de que el análisis se lleve a cabo (abierto vs. encubierto). Como se mencionó en las secciones iniciales, poner en conocimiento al personal suele ser adecuado, pero consecuentemente puede cambiar su comportamiento de tal manera que puede llegar a afectar los resultados de la evaluación. Por otra parte, no advertir al personal, puede dar lugar a que se adopten medidas que afectan innecesariamente el funcionamiento de la organización. Por ejemplo, un equipo de seguridad informática de la organización podría reaccionar ante un ataque externo cortando todos los accesos a los recursos y de esta manera afectar la actividad de análisis.

Si un objetivo es evaluar la respuesta del equipo de seguridad, u otras unidades operativas, entonces es claro que se deben aceptar los posibles riesgos y no poner sobre aviso al personal. También puede ser adecuado poner en conocimiento al personal de seguridad y dar instrucciones específicas para que ninguna acción sea tomada en respuesta a las pruebas. El equipo de analistas de seguridad, teniendo conocimiento del propósito y la motivación, debe ser capaz de realizar una propuesta adecuada a las necesidades de la organización. Para delimitar el alcance, se necesitan definir criterios de evaluación. En general, los criterios de evaluación utilizan métricas basadas en esfuerzo. Por ejemplo, se puede sugerir llevar a cabo N diferentes pruebas automatizadas + K pruebas manuales. Dichas métricas serán independientes de los resultados de las pruebas, es decir, independientemente de si detectan vulnerabilidades, se logra comprometer el objetivo de evaluación, o no se detecta nada. Los analistas de seguridad no deben asumir de antemano ningún tipo de hipótesis, deben analizar y brindar un diagnóstico a su cliente. Como toda

evaluación, la fiabilidad de dicho diagnóstico dependerá de la experiencia y del equipo de trabajo que lleva adelante las tareas. Ambas partes deben ser partícipes de la definición de objetivos y alcance del trabajo. El alcance del trabajo tiene que definir claramente lo que se debe o no debe hacer.

Algunos puntos importantes que el alcance debería cubrir son:

- El análisis se realizará sobre: la organización completa, una ubicación específica, una división específica, una subdivisión, etc.
- Tipo de análisis (caja negra o caja blanca, o combinación, por ejemplo).
- El análisis será abierto o encubierto.
- Análisis de infraestructura, de aplicación o ambos.

Luego de culminada la primera entrevista, el equipo de analistas que llevarán adelante las tareas, debe elaborar una propuesta, y para ello se tendrían que haber definido los siguientes puntos:

- Nombre y detalles de la persona a la que la propuesta debe ser presentada.
- El tiempo máximo para presentar la propuesta.
- El tiempo máximo, sugerido por la empresa, para completar la evaluación.
- Limitaciones horarias de la empresa para realizar el trabajo.
- Necesidad de firmar acuerdos de confidencialidad y responsabilidades.
- La propuesta, que presentará el equipo de analistas, debería incluir:
- Lo que se entendió de las necesidades/motivaciones de la organización cliente.
- Objetivos de la evaluación.
- Plazos del análisis de seguridad.
- Tiempo que insumirá cada tarea.
- Precondiciones para realizar el análisis de seguridad.
- Presupuesto y costo del análisis.
- Salvaguardas y período de mantenimiento de la oferta.

Algunas preguntas que el analista de seguridad debería hacer en una reunión inicial:

- *Alcance:* ¿qué se quiere evaluar? sitios web, aplicaciones, bases de datos, sistema de información interno o infraestructura en general.

- *El análisis:* ¿se pondrá en conocimiento a los administradores de TI que se están haciendo prueba de seguridad? o ¿se dejará que los tome por sorpresa?
- *Las pruebas*: ¿se podrán hacer pruebas todos los días y a todas horas (24x7)? ¿sólo los fines de semana? ¿entre semana a horas hábiles (8x5)? ¿o inhábiles?
- *Los acuerdos*: ¿quién firmará los permisos y documentos necesarios?, ¿se firmará un contrato de confidencialidad?, ¿la empresa ofrece uno?, ¿los analistas tienen uno?, ¿requiere que el departamento legal lo autorice?

5.3.1. Horarios y medidas de contingencias

Una vez que se acepta el presupuesto, se deben fijar nuevas entrevistas, un punto a discutir es sincronizar los horarios de trabajo (tabla de horarios). Es necesario establecer los días en los cuales los analistas podrán trabajar, y para cada día se define el momento de inicio y fin de las diferentes pruebas y etapas del proceso de evaluación. Definir la tabla de horarios es vital, ya que se asegura que, si bien se completarán las diferentes pruebas, las operaciones normales y cotidianas de la organización no serán interrumpidas. Posiblemente las pruebas necesiten ejecutarse en momentos concretos del día. Se deben evitar los conflictos entre la necesidad de asegurarse de que todo se pruebe y la necesidad de evitar la sobrecarga de los sistemas durante los períodos de usos críticos. Las pruebas que implican generación de tráfico de red inusual pueden causar que algunos sistemas se bloqueen o disparen alertas de falsos positivos. Si el riesgo no puede ser tolerado, es posible que algunos sistemas o redes tengan que ser excluidos del alcance de las pruebas. Los analistas de seguridad deben discutir y establecer adecuadamente los momentos en cuales se realizarán las pruebas, incluso antes de la elaboración de un plan de pruebas. No existen organizaciones que quieran que sus negocios se vean afectados por una evaluación de seguridad. Si el problema de la sincronización o puesta de acuerdo en horarios no se resuelve correctamente, esto podría ser catastrófico para la organización. Es necesario establecer desde donde se realizarán las pruebas, en el caso de que sea una evaluación externa, en la medida de lo posible, se debe indicar la dirección IP que se utilizará. En cualquier circunstancia, el analista debe llevar una bitácora, en ella se indicará la dirección IP que se utilizó, el tipo de tarea realizada y el horario de las pruebas.

Siempre que sea posible, es conveniente realizar las pruebas sobre una plataforma de desarrollo y luego constatarlas sobre la plataforma de producción. En cualquier caso, se deben tomar medidas para evitar contingencias.

Algunas de las medidas a adoptar son:

- Definir estrategias de contingencia para activos críticos.
- Si corresponde, involucrar al oficial de seguridad.
- Realizar respaldos de la información de los activos involucrados.
- Guardar en formato electrónico y físico las configuraciones de los equipos y las aplicaciones involucradas.
- Realizar monitoreo de los servicios durante las pruebas.
- Establecer políticas: ¿qué se hará si durante la prueba la operación se ve afectada (por ejemplo, con la caída de un servidor) ?, ¿quién tomará las decisiones de detener o continuar con la prueba?
- Establecer los canales de comunicación: ¿cómo se dará la comunicación entre las partes?, ¿telefónicamente?,¿por correo electrónico?, ¿se utilizarán canales cifrados?, ¿cuándo se intercambiará información?, ¿todos los días?, ¿final del día?

5.3.2. Equipo de trabajo

En esta sección se discutirán las funciones y responsabilidades de los miembros de un equipo de analistas de seguridad, también se planteará una posible manera de organizar un equipo de estas características.

Antes de comenzar a describir los roles, se enumerarán algunos criterios a tener en cuenta al momento de seleccionar personal para la realización de evaluaciones de seguridad. El criterio más importante para incorporar un analista de seguridad a un equipo de trabajo no es la habilidad técnica, ni su competencia, ni siquiera es la capacidad de comunicar los resultados, es simplemente la honradez. Sobre todo, si se tiene en cuenta que, cuando se permite que un analista de seguridad realice su trabajo, se está consintiendo el acceso a las computadoras y redes de la organización. El analista, explícitamente estará buscando el modo de violar los controles y obtener acceso a información sensible. De todas maneras, esto no quiere decir que no se tengan en cuenta otros criterios. Entonces, algunas pautas para seleccionar un analista de seguridad o un equipo serían:

Confiabilidad: ¿es la persona o el equipo seleccionado, digno de confianza para trabajar con la información sensible a la que potencialmente se podría acceder? Uno de los indicadores de confianza, suele ser la experiencia. Es difícil permanecer por mucho tiempo en el negocio de evaluaciones de seguridad, si no se es digno

de confianza. Un punto a tener en cuenta es no sólo concentrarse en las empresas consultoras de renombre. Estas empresas tienden a realizar evaluaciones genéricas, y las evaluaciones de seguridad son un trabajo especializado. Por último, hay que tener en cuenta que las certificaciones no evalúan la confianza, determinan a la habilidad técnica.

- *Disciplina:* El analista de seguridad debe permanecer dentro de las líneas de trabajo trazadas.
- *Competencia*: Es necesario utilizar correctamente la habilidad técnica, con el fin de encontrar vulnerabilidades.
- *Habilidad técnica:* Se debe entender la tecnología que se está evaluando.
- *Comunicación*: En necesario contar con la capacidad de expresar los resultados adecuadamente, de tal manera que la contraparte entienda las problemáticas.

Conseguir expertos en Seguridad Informática es una tarea difícil, es una profesión especializada, bastante nueva, y la demanda va en aumento. Si se agregan las pautas expuestas anteriormente, se torna aún más complejo. Por esta razón, se tiende a trabajar con equipos multidisciplinarios de analistas de seguridad. A continuación, se pasará a describir una posible composición de un equipo de esta naturaleza.

Dependiendo del alcance del proyecto y la estructura organizativa, la composición de un equipo de analistas de seguridad puede variar considerablemente. En general, se tendrán que cubrir los roles de: director de proyecto, auditor de seguridad, ingeniero de seguridad y documentador. No es absurdo pensar que múltiples roles dentro de la estructura, sean ocupados por la misma persona. A modo de ejemplo, el director de proyecto también podría actuar como ingeniero de seguridad cuando sea necesario, de igual manera un ingeniero de seguridad podría ser documentador del proyecto. Sin embargo, aunque se encuentren ocupados por el mismo individuo, los roles siguen existiendo. A continuación, la descripción de referencia para esos roles:

Director de proyecto

Incluir un director de proyectos mejora las posibilidades de éxito de una evaluación de seguridad. No es condición necesaria que el director de proyecto deba tener una comprensión detallada y específica de cada tarea que se realizará en una evaluación. Por el contrario, un error frecuente consiste en seleccionar un ingeniero de seguridad, con un perfil netamente técnico, como director del proyecto. Las tareas de director del proyecto son radicalmente diferentes a la de un ingeniero, el director

de proyecto debe de tener una formación adecuada en cuanto a gestión y, como se dijo anteriormente, no es necesario que tenga conocimientos específicos de las tecnologías subyacentes. El individuo que ocupe este rol debe ser competente para planificar, organizar y administrar la ejecución del proyecto. Es imperioso que tenga capacidad de dirección, liderazgo y toma de decisiones. Necesita aptitudes para la negociación, para el trabajo en equipo y la motivación del personal. Debe estar familiarizado con los diferentes tipos de evaluaciones de seguridad y las tareas que se ejecutan. A modo de ejemplo, y sin ánimo de brindar una lista completa, se listarán para cada rol algunas de las actividades en las que están involucrados.

A continuación, se listan algunas de las actividades en las que está involucrado el director de proyecto:

- Construir la credibilidad del equipo de trabajo.
- Coordinar la propuesta económica.
- Establecer la relación contractual.
- Dirigir el equipo de trabajo.
- Comprender y evaluar riesgos.
- Detectar asunciones sin especificar y resolver conflictos.
- Anticiparse a los problemas.
- Establecer los canales de comunicación.
- Establecer los puntos de contacto ante contingencias.
- Tomar las decisiones necesarias para lograr los objetivos establecidos.
- Organizar y supervisar la ejecución de las actividades.
- Coordinar las reuniones internas del equipo, y las externas (con la organización).
- Planificar el cierre de la evaluación.

En general con un director por proyecto es suficiente, y dependiendo de la envergadura de los proyectos, un mismo director podría estar gestionando más de un proyecto al mismo tiempo.

Auditor de Seguridad

Un auditor se encarga de evaluar acorde a criterios establecidos, y la mayor parte de las veces siguiendo una metodología concreta, es capaz de determinar cuáles son los niveles de cumplimiento con los objetivos marcados por esos criterios.

El auditor, verifica que las actividades en las organizaciones se realicen de forma adecuada, y que las normas se cumplan, por esta razón necesitan que su carácter sea extrovertido. En general, y por la naturaleza de sus tareas, se encarga de entrevistar a diferentes actores dentro de la organización y documentar los objetivos de seguridad que persigue una organización cuando se solicita una evaluación de seguridad. Para llevar sus tareas adelante, debe estar debidamente entrenado y poder reconocer los síntomas superficiales que le advierten de la existencia de problemas. Necesita contar con conocimiento de normas profesionales y legales, experiencia en el manejo de temas operativos y de gestión. Debe tener amplitud de criterios, estar acostumbrado a tratar los temas con una visión global y no sujetarse a reglas muy rígidas. Sobre todo, necesita sensatez de juicio y sentido común.

Actividades en las que está involucrado un auditor:

- Planear y administrar las tareas de auditoría.
- Recopilar la información necesaria para el control integral e integrado.
- Mantener una relación fluida y continua con los sectores auditados.
- Lograr un conocimiento acabado de las políticas, metas y objetivos de la organización evaluada.
- Revisar planes de seguridad y contingencia.
- Revisar el cumplimiento de los procedimientos.
- Revisar controles relativos a seguridad física.
- Revisión de las políticas relacionadas.
- Evaluar riesgos.
- Analizar los procedimientos para la realización de las copias de seguridad.

Ingeniero de Seguridad Informática

Los ingenieros de seguridad informática no deben ser vistos como auditores, ambos roles requieren conjuntos de competencias diferentes y en general realizan tareas complementarias. A menudo existen diferencias en el modo de proceder de cada uno, frecuentemente los auditores piensan a la defensiva, mientras que los ingenieros de seguridad en la ofensiva. Son perfiles distintos, que hacen trabajos distintos, y no por ello uno es más valioso que el otro. Cuando se comienza a trabajar, el conjunto de habilidades de los ingenieros de seguridad (también llamados pentester) y los auditores, debe corresponderse con los objetivos identificados

y el software/hardware utilizado en la organización a evaluar. A un ingeniero de seguridad podría no importarle cual es el cumplimiento de los objetivos y que tanto se apega la organización a los procedimientos. Su tarea es buscar vulnerabilidades en los sistemas y explotarlas, muchas veces independientemente de los procesos que rodean el sistema y por lo tanto, requiere de un mayor nivel de conocimiento de dichos sistema.

El ingeniero de seguridad informática es un experto en seguridad de sistemas con el instinto y conocimientos de un atacante. Tiene que ser capaz de pensar como un atacante y debe conocer cuáles son las metodologías y las herramientas utilizadas. Debe tener amplios conocimientos en lo que respecta al manejo de diferentes sistemas operativos, telecomunicaciones, aplicaciones y vulnerabilidades. Necesita conocimientos de programación para la creación de herramientas y código para explotar vulnerabilidades. Debe ser capaz de procesar y realizar las diferentes pruebas de manera sistemática, crear documentación, escribir reportes y presentar los resultados de sus investigaciones a técnicos y no técnicos. Dada la gran cantidad de sistemas y tecnologías existentes, cada experto se puede especializar en un dominio particular o en un área específica. Consecuentemente, podrá asesorar en cuestiones sobre las que posee un conocimiento especializado. Acorde a una problemática, o a un deseo de mejora en el área de la seguridad, será capaz de plantear una serie de soluciones que permiten conseguir los objetivos.

Actividades en las que está involucrado un ingeniero de seguridad:

- Actuar y pensar como un atacante.
- Realizar pruebas sobre: dispositivos de red principales servidores estaciones de trabajo y aplicaciones
- Descubrir y analizar vulnerabilidades, en forma manual y automática.
- Programar herramientas para atacar los objetivos.
- Planificar y ejecutar estrategias de ataques.
- Poner al descubierto los riesgos existentes

La cantidad de ingenieros de seguridad y auditores depende de la complejidad de la evaluación. Podría llegar a existir más de un ingeniero por cada área a evaluar, a modo de ejemplo: expertos en bases de datos, en sistemas operativos y expertos en aplicaciones web. La experiencia en un área no es el único factor determinante al momento de asignar ingenieros de seguridad a un proyecto, también están los tiempos que se hayan acordado con la organización. Hay que tener en cuenta que

cuantos menos ingenieros, menos capacidad tendrá el equipo para paralelizar las tareas de campo.

Documentador

Es el responsable de confeccionar los materiales a entregar a la organización, basándose en los estándares definidos y en los requerimientos relevados. Esto incluye crear presentaciones, notas, ejemplos y todos los materiales que faciliten el entendimiento de la evaluación, ya sean estos partes de los entregables o porque se considere pertinente contar con los mismos. Debe tener experiencia en el desarrollo de materiales, conocer y entender muy bien las metodologías de evaluaciones de seguridad. Para poder transmitir los problemas en términos conocidos por el usuario final (sean estos técnicos o no), debe involucrarse con el modelo/realidad de negocios de la organización evaluada.

Actividades en las que está involucrado un documentador:

- Elaborar propuesta de trabajo y participar en la propuesta económica.
- Gestionar la documentación de la relación contractual.
- Gestionar los acuerdos de confidencialidad y responsabilidad.
- Generación y verificación de todos los entregables.
- Solicitar evidencia de ataques a los ingenieros de seguridad.
- Registrar el esfuerzo.
- Elaborar la presentación de la evaluación.

Para este rol se puede asignar una persona como documentador principal y en la medida que se vayan desvinculando de sus tareas se pueden incorporar alguno de los ingenieros y/o auditores a tareas de documentación.

5.2. Especificación de una Evaluación de Seguridad

Según la definición de objetivos y la posición en la que se ubiquen los analistas de seguridad, se podrán aplicar diferentes técnicas. Muchos tipos de pruebas requieren que los analistas puedan operar sobre un determinado equipo o host, otras se pueden realizar en forma remota desde la red. También se tiene que considerar si se desea analizar la infraestructura, las aplicaciones, una base de datos o todo lo anterior. Cuando las evaluaciones son realizadas por terceros, la organización tendrá que determinar el nivel apropiado de acceso físico que se dará a los evaluadores (por

ejemplo, acceso sin restricciones o acompañado). Asimismo, uno de los objetivos puede ser evaluar la seguridad física de la organización.

Para las evaluaciones técnicas realizadas dentro de la red, tales como las revisiones de configuración y escaneo de vulnerabilidades, es conveniente que los analistas tengan acceso a la red ya sea en el sitio, a través de una red privada virtual (VPN) o a través de una conexión dedicada.

Los evaluadores pueden requerir diferentes niveles de acceso a la red en función de las herramientas que utilizan. Algunas herramientas requieren privilegios de administrador, por ejemplo, las herramientas orientadas a auditoría. Si este es el caso, las organizaciones deben crear nuevas cuentas de administrador, que se utilizarán únicamente durante las evaluaciones. Cada evaluador debe tener su propia cuenta en el sistema, los usuarios no deben ser compartidos. Este enfoque permite que la organización pueda supervisar dichas cuentas.

A continuación, se describen algunos de los análisis específicos que se podrían llegar a desarrollar en una organización. No pretende ser una descripción exhaustiva ni completa, pueden existir otros enfoques. Lo que se pretende es orientar al lector y brindar una de las posibles maneras de concebir los diferentes tipos de evaluaciones de seguridad, introduciendo la noción de "posicionamiento", es decir, la ubicación que puede tomar un analista de seguridad al momento de llevar adelante sus tareas.

5.2.1. Evaluación de una red

En este tipo de análisis los evaluadores generalmente se posicionan dentro de la red de la organización, en general se brinda una dirección IP dentro de la institución y los analistas llevan su propio equipamiento para conectar en la red. Esta ubicación permite que el analista pueda realizar su tarea como si se encontrara en un puesto de trabajo. Las tareas típicas para ejecutar son la de monitoreo de tráfico, descubrimiento de red, identificación de puertos y servicios, escaneo de vulnerabilidades, y todas las técnicas que se puedan realizar sobre los equipos que se encuentren dentro del radio de acción. Asimismo, mediante la explotación de vulnerabilidades se puede intentar ganar el acceso a servidores de la organización en forma remota.

5.2.2. Evaluación de un equipo o host

Aquí el objetivo es analizar un determinado host, puede ser una estación de trabajo, un servidor o un dispositivo de red determinado. En general, la organización brindará al equipo de analistas uno o varios usuarios en el sistema operativo del host a evaluar.

Los usuarios que se brindan a los analistas en general tienen diferentes privilegios. Puede ser adecuado que a un ingeniero de seguridad se le facilite un usuario con mínimos privilegios, y mediante diferentes técnicas, se intentará lograr ganar mayores niveles de acceso o escalar privilegios.

Un auditor puede requerir un usuario que tenga privilegios de administrador, de esta manera se utilizarán herramientas que permitan evaluar diferentes características del sistema. A modo de ejemplo se pueden evaluar las políticas de cambio de contraseña, las actualizaciones que están instaladas en el sistema, revisión de bitácoras, entre otros.

El análisis de red y el análisis de host son tareas complementarias. Un caso típico, es que un analista no logre el acceso remoto al sistema operativo de un host por tener un firewall local, pero el sistema si tiene vulnerabilidades que sólo son accesibles mediante usuarios locales.

5.2.3. Evaluación de aplicaciones

En los dos tipos de evaluaciones mencionadas anteriormente se realizan tareas enfocadas a la infraestructura, por ejemplo: sobre sistemas operativos, sobre aplicaciones de base (servidores web o de correo electrónico). El analista de seguridad se ubica en la red o en determinado host.

Debido al auge de las aplicaciones web, cuando se hace referencia al término análisis de aplicaciones, en general se asume que se está hablando de este tipo de aplicaciones. Si bien el análisis de aplicaciones web es lo más habitual, también se pueden realizar diferentes tipos de análisis a otro tipo de aplicaciones, por ejemplo: aplicaciones de control de stock o de ventas que no se accedan mediante una interfaz web.

Aquí se pueden tomar dos enfoques, uno de ellos similar a un análisis de red, en donde el analista de seguridad no cuenta con ningún tipo de credenciales en el sistema o aplicación. El otro enfoque, al igual que en un análisis de host, se brinda a los analistas usuarios con diferentes niveles de privilegios.

Independientemente del enfoque, el ingeniero de seguridad que se encargue de evaluar la aplicación tratará de descubrir vulnerabilidades y lograr acceso con mayores niveles de privilegios. Para ello, es necesario estudiar la lógica de negocios de la aplicación, también se buscarán las vulnerabilidades típicas, por ejemplo: inyección de SQL, Cross Site Scripting, contraseñas débiles, entre otros.

Un auditor de seguridad también podría trabajar sobre la aplicación. Puede evaluar los diferentes tipos de controles y los mecanismos que tenga la aplicación en lo que refiere a la seguridad. Por ejemplo, puede verificar los mecanismos de identificación y autentificación, la existencia de roles, controles en las transacciones, limitaciones de servicio, modalidad de acceso, etc. Si se cuenta con el código de la aplicación, también se puede hacer una auditoría de este.

5.2.4. Evaluación de bases de datos

Los Sistemas de Gestión de Bases de Datos (SGBD) en general son los recursos más importantes que una organización posee. Aquí se almacenan datos de clientes, información financiera, información de recursos humanos, los datos de los negocios de la organización y otros. Consecuentemente es muy importante realizar un análisis de dichos motores de bases de datos.

Un caso típico es que los datos que se encuentran en la base de datos sean accedidos mediante una aplicación. Dicha aplicación puede manejar diferentes roles, tener controles de seguridad y demás, pero ¿qué sucede si se accede directamente al motor de base de datos?, ¿los controles son los adecuados?

La tarea del ingeniero de seguridad podría ser la de prescindir de las aplicaciones e identificar el motor de bases de datos subyacente, para luego intentar obtener los datos mediante la explotación de una vulnerabilidad. También puede aplicar técnicas de fuerza bruta para intentar obtener algún tipo de credencial de acceso.

Un auditor podría evaluar los parámetros de instalación del SGDB, los tipos de usuarios, perfiles y privilegios necesarios para controlar el acceso a la base de datos, mecanismos de respaldo o si se están utilizando las funcionalidades de seguridad provistas por el SGBD.

5.2.5. Evaluación de la seguridad física

La seguridad física describe las medidas que previenen o disuaden a los atacantes para impedir que tengan acceso a un edificio o centro de cómputo, un recurso o a información almacenada en soportes físicos. Puede ser tan simple como una puerta cerrada con llave o tan elaborada como contar con múltiples niveles de acceso físico, controles biométricos y oficiales de seguridad.

Un ingeniero de seguridad podría intentar evadir los controles y acceder a los servidores de una organización. En general, para esta tarea, se utilizan técnicas de

ingeniería social y salvo un pedido explícito de la organización no se llevan adelante este tipo de ataques.

Por otro lado, puede ser pertinente realizar una evaluación de la seguridad física. A modo de ejemplo, un auditor podría:

- Determinar si la sala de informática está equipada con cerradura para limitar el acceso, que los dispositivos y cuentas de acceso están debidamente asignados.
- Comprobar si las llaves o tarjetas magnéticas, tienen un control de inventario y si se devuelven cuando un individuo deja el empleo o se mueve a otro departamento.
- Determinar los diferentes niveles de acceso que proveen las tarjetas, o cuentas de acceso. Cada función o cargo, debe tener un único nivel de acceso físico, de acuerdo con las responsabilidades.
- A través de la observación, determinar si las puertas de la sala de informática se mantienen cerradas en todo momento.
- Verificar los mecanismos de seguridad física previstos para desastres.

5.2.6. Análisis de vulnerabilidades

El análisis de vulnerabilidades o proceso de evaluación de vulnerabilidades consiste en: identificar, evaluar y categorizar vulnerabilidades de seguridad en sistemas en un momento dado. Cuando se ofrece el servicio de análisis de vulnerabilidades, generalmente se refiere a un servicio basado parcial o totalmente en herramientas automatizadas que hacen gran parte del trabajo pero que también se hace necesario la revisión de manual cuando surgen algunas dudas. La información proporcionada por las herramientas es comparada con una base de datos de vulnerabilidades conocidas. Como resultado del servicio, se obtiene un listado de fallos de seguridad, que en ocasiones se encuentran ordenados según un índice de criticidad.

Si bien se utilizan principalmente herramientas automatizadas, el analista de seguridad es el encargado de descartar los falsos positivos generados por las herramientas. También evalúa las vulnerabilidades, y dependiendo de los activos de la organización en cuestión, les asigna un nivel de riesgo y prioridad. Para este tipo de evaluación, el trabajo se focaliza en el impacto potencial que las vulnerabilidades podrían tener en la organización.

En general, como parte del resultado una Evaluación de Seguridad, el equipo de analistas de seguridad puede recomendar a la organización soluciones a las vulnerabilidades encontradas, e incluso diseñar un plan de acción.

5.2.7. Pruebas de intrusión

Conocido popularmente como una prueba de penetración (o intrusión), es esencialmente una evaluación de seguridad, en un momento dado, de un determinado sistema. Como resultado del servicio, se tiene una estimación del éxito que podría tener un agente malicioso, o usuario malintencionado, al atacar dicho sistema. Dicho de otra manera, se tiene una medida de que tan susceptible se encuentra el sistema frente a las acciones de atacantes maliciosos.

El proceso consiste en la enumeración y análisis de cualquier defecto técnico o vulnerabilidad. Después de verificadas las vulnerabilidades, se las aprovecha para hacer intentos de infiltración sobre el sistema, de esta manera se busca ganar algún tipo de acceso. Una vez que se ingresa al sistema objetivo, se busca escalar privilegios para obtener mayores niveles de acceso, en lo posible se intenta lograr los privilegios de administrador del sistema.

En el proceso, el equipo de analistas de seguridad trata de descubrir las vulnerabilidades en los sistemas utilizando tanto herramientas automatizadas, como manuales. Se recopilarán evidencias de los accesos, de los fallos de seguridad que se encuentren en los sistemas y cuya seguridad haya sido vulnerada.

Un punto importante para destacar es que mientras el análisis de vulnerabilidades tiene como objetivo identificar las vulnerabilidades de los sistemas, una prueba de intrusión va un paso más allá, y tiene como objetivo demostrar cómo éstas pueden ser utilizadas por potenciales agentes maliciosos. En este caso, el foco de las tareas es ganar acceso a los sistemas y/o información sensible de la organización o sus clientes.

Hay que tener en cuenta que los resultados están expresados en función del tiempo dedicado por los analistas de seguridad y la pericia de estos.

Una Prueba de Intrusión puede ser útil para determinar:

- La tolerancia de los sistemas objetivos ante la realización de patrones de ataque reales.
- El nivel de habilidad que un atacante necesita para poder comprometer el sistema.

- Contramedidas que se pueden adicionar al sistema para disminuir las amenazas posibles.
- La habilidad de los defensores para poder detectar y responder ante incidentes de seguridad perpetrados contra el sistema.

Una prueba de Intrusión es de suma utilidad cuando se realiza una Evaluación de Seguridad de un sistema o una red, pero requiere mucho esfuerzo y habilidad a fin de minimizar los riesgos que se le pueden hacer correr al sistema objetivo. Los sistemas pueden ser dañados, o tornarse inusables, en el transcurso de la ejecución de una prueba de este tipo. Aunque los responsables de realizar las pruebas sean muy experimentados el riesgo persiste, por lo tanto, la decisión de realizar una evaluación de este tipo debe ser cuidadosamente considerada, notificada y planificada.

Al igual que en el análisis de vulnerabilidades el equipo de analistas de seguridad puede recomendar a la organización soluciones para las vulnerabilidades encontradas e incluso diseñar un plan de acción para solucionarlas.

5.2.8. Auditorias de seguridad

Una auditoria de seguridad, al igual que las actividades descritas anteriormente, consiste en: identificar, evaluar y categorizar vulnerabilidades de seguridad en sistemas. Es un proceso más exhaustivo que un análisis de vulnerabilidades y generalmente abarca el análisis de: estaciones de trabajo, redes de datos, servidores, políticas de seguridad, manejo de información, entre otras.

Una auditoría es un concepto mucho más general, se puede evaluar la eficiencia, el rendimiento, la escalabilidad, la compatibilidad, los tiempos de recuperación ante un incidente de seguridad. La auditoría evalúa habitualmente una o varias características de los sistemas, así como su interrelación. Dichas características ni tan siquiera tienen por qué ser técnicas, es posible auditar aspectos operacionales.

Generalmente, un análisis de seguridad se realiza con base en un criterio conocido o conjunto de directrices o buenas prácticas sugeridas. Existen estándares orientados a servir como base, por ejemplo: COBIT (Objetivos de Control de la Tecnologías de la Información) y los estándares de la familia ISO 27000.

Abarca tanto la seguridad física como la seguridad lógica. La seguridad física hace referencia a la protección de hardware, así también como la seguridad de las instalaciones que lo albergan. Por otra parte, la seguridad lógica se refiere a la

seguridad en cuanto al uso de software, mecanismos de protección de información y procesos. También hace referencia a lo que refiera a autorización y autenticación.

A modo de ejemplo, en lo que refiere a sistemas operativos y aplicaciones se pueden realizar tareas que verifiquen la existencia de vulnerabilidades, así como también una revisión de configuraciones. Dicha revisión evalúa si las configuraciones son apropiadas y están de acuerdo con las necesidades de la organización, proporcionando así un control adecuado y robusto para asegurar propiedades como: confidencialidad, integridad y disponibilidad del sistema.

En cuanto a las políticas, se podría evaluar si la organización tiene:

- Una política de privacidad.
- Una política de acceso.
- Una política de autenticación.
- Una política de mantenimiento para la red.
- Una política de divulgación de información.
- Una política de respaldos.

En una evaluación de seguridad se podrían incluir entrevistas de relevamiento con diferentes interlocutores de la organización, siguen una modalidad abierta (el personal es consciente) y de caja blanca. Aunque en ocasiones pueden trabajar varios equipos de analistas de seguridad, unos enfocados al relevamiento y otros realizando tareas de pruebas de penetración o análisis de vulnerabilidades.

Una auditoría, salvo que el alcance no lo requiera, puede perfectamente incorporar una prueba de penetración como una prueba más.

5.2.9. Establecimiento de relación contractual

En muchos casos, un análisis completo implica que los analistas de seguridad realicen actividades ilegales en sistemas internos o externos a la red de una organización. Las organizaciones deben entender esta problemática y es tarea del equipo de analistas hacer explícito este hecho. En general existen dos tipos de acuerdos a firmar entre las partes, uno que protege a la organización que solicita el servicio y otra que protege a los analistas y a la organización que realiza las tareas. Ambos acuerdos deben ser impresos en papel, con membrete de la empresa y firmado por una persona responsable dentro de la organización.

5.2.10. Acuerdo de confidencialidad

Es vital asegurar que la organización entienda que cualquier información o dato obtenido durante las pruebas será tratado como confidencial y será devuelto o destruido luego de concluido el análisis. Para ello es necesario firmar los acuerdos de confidencialidad correspondientes (NDA, por sus siglas en inglés). Esta información puede incluir datos de la infraestructura, información crítica de los clientes, secretos comerciales e información personal de los empleados de la organización. La revelación de esta información podría tener un impacto negativo en la imagen de la organización o, peor aún, si la información cae en manos de agentes mal intencionados podría ser utilizada indebidamente para un ataque localizado.

En general, se puede establecer tres tipos de acuerdo:

- *Completo*: toda información completa o parcial, en relación con las tareas, no puede ser distribuida o utilizada como material de investigación, capacitación o comercialización.
- *Limitado*: cierta Información limitada puede ser utilizada en escenarios de formación y capacitación, investigación y marketing, la organización es quien decide qué información puede ser utilizada.
- *No restringido*: toda la información es de libre distribución y no hay ningún tipo de restricción.

Un acuerdo de confidencialidad debe incluir:

- Propósito.
- Responsabilidades.
- Devolución y mecanismos de destrucción de datos y materiales (soporte físico de la información).
- Restricciones de uso, transmisión y reproducción.
- Licenciamiento.
- Términos de uso y plazos del acuerdo.
- Ley aplicable y la jurisdicción.
- Enmiendas frente a daños.

El acuerdo debería incluir capturas de pantalla, la documentación generada (incluidos todos los borradores, así como la versión final), cualquier e-mail intercambiado con la

organización, los manuales obtenidos, los planes de negocio, información financiera, y cualquier cosa que tuviera que ver con el proyecto.

El equipo de analistas de seguridad también debe entender que cuando firma un NDA no sólo asume la promesa de mantener la confidencialidad de los datos de su cliente durante el transcurso de las pruebas, también asume la promesa de mantener la confidencialidad todo el tiempo que los tenga en su poder, es decir, hasta que estén destruidos de acuerdo con el calendario y método establecido. Cuando se firma un acuerdo de confidencialidad no es simplemente un acuerdo para no hablar de los activos de las organizaciones, es un acuerdo para mantener, bajo llave, todos los datos relacionados con la actividad. Con o sin el acuerdo de confidencialidad, los analistas de seguridad están éticamente obligados a mantener la confidencialidad y garantizar la no divulgación de la información del cliente, ni los resultados del análisis.

5.2.11. Acuerdo de responsabilidades

Para realizar un análisis de seguridad es necesario obtener una autorización clara de la organización. Por lo general, la aprobación debe ser tratada de tal manera que la organización asume la responsabilidad de los resultados y los efectos secundarios del análisis (si existieren). Es muy importante que quien otorgue los permisos sea la persona adecuada, claramente la gerencia tiene que intervenir en el proceso. En este contexto, compromisos y documentos legales que protejan a los analistas de seguridad y la empresa que representan también deben estar firmados antes de comenzar las tareas en una organización. Este es un punto importante, no se debe descuidar y es lo primero que hay que hacer. Incluso si los analistas son parte del personal de la organización, se deben firmar los documentos jurídicos que los proteja contra cualquier acción legal.

Este tipo de acuerdos sirve como una protección para los analistas por si algo sale mal durante las pruebas. Los accidentes pueden ocurrir y a un analista no le gustaría ser demandado como resultado de hacer su trabajo. De todas maneras, los analistas siempre deben asumir parte de la responsabilidad y esto se traduce en una cifra económica, en general el monto aceptable de dicha responsabilidad es igual al costo del servicio. Esto debería incluir errores no intencionados y un posible mal manejo de herramientas, aun cuando los analistas deben conocer sus herramientas, como trabajan, y siempre haberlas probado en un área restringida antes de usarlas en la infraestructura del cliente.

5.2.12. Limitaciones contractuales y dinámicas operativas

Los contratos deben explicar claramente los límites y peligros de un análisis de seguridad y debe incluir permisos claros y específicos para análisis que involucren negación de servicio o ingeniería social. Los contratos deben contener cláusulas para contratos futuros y cambios en las condiciones de trabajo. Es importante dentro de las limitaciones explicar claramente los límites del análisis de seguridad.

El plan de trabajo debe incluir tanto tiempo calendario como horas-hombre. Si es necesario para pruebas con privilegios, el cliente debe proveer dos mecanismos de acceso independientes, ya bien sean nombres de usuarios y contraseñas, certificados, números de identificación, entre otros. Estos deben tener los privilegios típicos de los usuarios a ser analizados por lo que no se recomienda utilizar cuentas especiales o aseguradas. En el caso de análisis remoto, el contrato debe incluir el origen de las pruebas por número telefónico y/o direcciones IP.

Vulnerabilidades de alto riesgo, como huecos de seguridad, vulnerabilidades con alta tasa de explotación, explotables y que permitan acceso total no monitoreado, sin dejar rastro o que puedan poner en peligro vidas y que sean descubiertas durante el análisis, deben ser reportadas al cliente con una solución práctica tan pronto sean encontradas. Las notificaciones al cliente son requeridas cuando el analista cambie el plan de trabajo, cambie el origen de los análisis, obtenga resultados de alto riesgo, con antelación a la ejecución de nuevos análisis de alto riesgo y alta generación de tráfico, y en caso de que hayan ocurrido problemas en el análisis.

Adicionalmente el cliente debe ser notificado con reportes de progreso semanalmente, debe ser informado del envío de informes y debe confirmarse la recepción de este. Todos los canales de comunicación para la entrega de información deben ser confidenciales pues la información que se intercambie podrá contener datos sensibles para la organización e incluso para el mismo analista de seguridad. Se deben definir los criterios de aceptación de resultados y los responsables de aceptar o rechazar esos criterios.

5.3. La ejecución de tareas

5.3.1. Reconocimiento

El término reconocimiento es utilizado habitualmente en la jerga militar y refiere a las misiones para obtener información de un objeto de evaluación mediante la aplicación de diferentes métodos. La finalidad principal se centra en producir

información táctica que, luego de evaluada, se utilizará para confirmar, modificar o elaborar planes estratégicos.

Para ilustrar la situación, se podría plantear la analogía con un delincuente que quiere efectuar un atraco en una determinada casa. El delincuente podría irrumpir sin ningún tipo de información, o podría dedicar tiempo a observar los movimientos y horarios de los propietarios (merodeo), inferir la cantidad de moradores de la casa, la existencia de mecanismos de seguridad y de esta manera planear sus movimientos y estrategias.

El reconocimiento es la etapa inicial dentro de la fase de ejecución de tareas y es esencial que sea realizada. El objetivo principal es recopilar toda la información que sea posible, ya que la misma es importante tanto para planificar los siguientes pasos, como para informar a los destinatarios cuál es la información sensible que se puede recuperar de sus sistemas, infraestructura o bases de datos.

Dependiendo del tipo de análisis de seguridad (caja negra, caja blanca o caja gris), el modo de operación puede consistir en emular las técnicas que utilizan los atacantes para obtener información. La recopilación de información se realiza esencialmente mediante el uso de Internet empleando diferentes métodos técnicos como pueden ser, entre otros: consultas a sistema de nombre de dominios (DNS), sistemas de consulta WHOIS (no es un acrónimo), consultas en motores de búsqueda, grupos de noticias, listas de correo, análisis de metadatos de archivos, entre otros.

También se pueden aplicar técnicas de revisión, donde se analicen políticas y procedimientos, configuraciones de sistemas y logs de dispositivos, para luego elaborar estrategias y tácticas de ataque que se validarán en etapas sucesivas.

En general, en esta etapa se utilizan métodos de acceso indirectos. No se requiere que los analistas de seguridad establezcan contacto con los objetos de evaluación, la principal finalidad es obtener información sin ocasionar sospechas, ni levantar alarmas, como, por ejemplo, aquellas generadas por los sistemas de detección de intrusos (IDS). En esta línea, una de las disciplinas a destacar es la de obtención de información y elaboración de inteligencia a partir del contenido de fuentes públicas para este fin, conocidas como Open Source Intelligence (OSINT).

5.3.11. Técnicas y herramientas

En lo siguiente se supone un análisis de caja negra, donde el analista se encuentra en condiciones similares a las de un atacante. Se enumera una serie de herramientas

utilizadas en la etapa de reconocimiento, las que se encuentran disponibles en Internet y son de acceso público.

Consultas WHOIS: un punto de partida natural, en la etapa de reconocimiento, es averiguar todo lo que se pueda acerca de la red en la que se encuentra el objeto de evaluación. Se busca información acerca de los responsables, los administradores y los técnicos. En este sentido, WHOIS es un protocolo que se encuentra definido en el Request for Comments 3912 (RFC3912), es un protocolo basado en TCP y orientado a un esquema de petición/repuesta. Este protocolo se utiliza para proporcionar servicios de información a los usuarios de Internet. Un servidor WHOIS escucha las solicitudes de los clientes en el puerto TCP 43 y la respuesta que brinda se encuentra en lenguaje natural y puede contener más de una línea de texto.

La respuesta contiene información sobre los datos registrales de determinado dominio, de manera similar a una guía telefónica. La principal crítica al protocolo es que aparecen todos los datos de contacto de quien registra el dominio, incluyendo números de teléfono y direcciones.

La Internet Corporation for Assigned Names and Numbers (ICANN), es un organismo independiente, sin fines de lucro, creado en 1998 con el objeto de coordinar la asignación global de identificadores que deben ser únicos en Internet tales como el espacio de direcciones IP, el sistema de asignación de nombres de dominio y la definición de parámetros de los protocolos utilizados. En virtud de las políticas y los contratos con la ICANN, las empresas que ofrecen servicios de registro de dominios deben ofrecer un servicio de WHOIS público.

No existen servidores WHOIS que contengan información centralizada, ICANN delega a otras entidades lo relacionado con el registro de domino, en particular para Latinoamérica la Latin America and Caribbean Network Información Centre (LACNIC) es la encargada regional. A su vez, la LACNIC delega a entidades locales.

Consecuentemente, los analistas de seguridad necesitan encontrar los servidores a los cuales tiene que realizar la consulta específica. La Internet Assigned Numbers Authority (IANA), que era el antiguo registro central de los protocolos Internet y fue sustituido en 1998 por ICANN, brinda en su sitio web una lista de empresas que ofrecen servicio de registro de dominios.

Existe una amplia gama de herramientas que se pueden utilizar para realizar consultas a servidores WHOIS, en particular en los sistemas UNIX se encuentra el comando de

consola whois y hoy por hoy se pueden encontrar muchos enlaces en Internet de sitios que ofrecen este servicio de forma gratuita.

Consultas DNS: otra fuente de información importante en la etapa de reconocimiento son los datos que se puedan obtener mediante consultas al servicio DNS (Domain Name System). DNS es un sistema que permite la traducción de nombres de dominio a direcciones IP y viceversa, es un sistema distribuido, jerárquico y replicado. DNS utiliza un esquema cliente servidor, los servidores de nombres de dominios contienen la base de datos de un segmento y dicha base de datos es accedida por los clientes. Una vez conocido el nombre de dominio del objetivo (o una dirección IP), se pueden realizar consultas a servidores DNS para obtener información de dominio público.

A continuación, se enumeran algunos de los datos que se pueden obtener:

- *Datos del proveedor de servicios DNS:* comprobando quien es el proveedor de servicios se podrá deducir si el servidor está alojado en instalaciones del objetivo o si se subcontrata el servicio. Si está alojado en las instalaciones del objetivo, el servicio DNS puede ser un blanco de ataques entrantes, y la seguridad dependerá de la experiencia de los administradores que se encuentren a cargo.
- *Nivel de aislamiento de las transferencias de zona*: una transferencia de zona es el término utilizado para hacer referencia al proceso mediante el que el contenido de un archivo de zona DNS se copia desde un servidor DNS principal a un servidor DNS secundario. Es una función completamente legítima de un servidor DNS, pero si está disponible a cualquier extraño, se podría obtener una lista de todos los equipos registrados en el dominio del objetivo. Si todo está bien configurado la mayoría de los intentos de transferencia de zona producirán un error, el problema radica cuando los nombres de dominios públicos y privados están en el mismo servidor DNS. En dicho caso, y si se permite la transferencia de zonas, se podrían obtener datos de la red interna y al obtener esto, sería el equivalente a obtener un mapa de toda su topología de su red. En caso de no soportar transferencias de zona se podrían aplicar técnicas de fuerza bruta para obtener información.
- *Registros y nombres de servicios particulares*: consultando ciertos registros y nombres comunes en el servidor DNS, se podrá identificar si se subcontrata el servicio o si está en servidores propios del objetivo.
- *Name Server (NS):* indica los servidores de nombres autorizados para la zona. Cada zona debe contener registros indicando tanto los servidores principales

como los secundarios. Por lo tanto, cada zona debe contener, como mínimo, un registro NS.

- *Mail eXchange Record (MX):* es un recurso DNS que especifica cómo debe ser encaminado un correo electrónico en Internet. Los registros MX apuntan a los servidores a los cuales se envían los correos electrónicos.
- *Nombres comunes*: Dependiendo de la infraestructura, generalmente existen equipos que podrían contener servicios que se pueden convertir en eventuales blancos de ataques, ejemplos de nombres son: 'www', 'www1', 'prueba', 'correo', 'pop', 'imap', 'webmail' y similares. Generando diccionarios, se podrían realizar consultas mediante fuerza bruta, para identificar dichos nombres de equipos y/o subdominios.
- *Consultas en motores de búsqueda*: si nos referimos a consultas en Internet, los buscadores son herramientas muy populares y necesarias, se han desarrollado técnicas que los hacen cada vez más potentes, consumen información de múltiples fuentes para potenciar las búsquedas, prácticamente sin importar el formato en el que estén almacenados.

Al momento de buscar material, estas herramientas ayudan a que se disponga de grandes volúmenes de información sobre determinado tópico. Por otro lado, también posibilita que se acceda a información sensible que no ha sido debidamente asegurada.

En particular el uso del buscador Google se ha masificado y pone a disposición de los usuarios múltiples opciones de búsqueda. Dichas búsquedas van desde las más sencillas, hasta las más poderosas que hacen uso de comodines de búsquedas, operadores lógicos, y los denominados operadores avanzados.

Al igual que los usuarios comunes, los analistas de seguridad han potenciado su trabajo incorporando técnicas de búsquedas en la etapa de reconocimiento de un objetivo, tal como el llamado Google Hacking el cual hace referencia a la capacidad de crear búsquedas, especialmente construidas para Google, cuyo objetivo es identificar, en forma pasiva e indirecta, servidores vulnerables, datos confidenciales, entre otros. En este sentido, no se puede dejar de hacer referencia a Johnny Long, un experto estadounidense en seguridad informática, autor de múltiples libros de seguridad y precursor de Google Hacking.

Long crea lo que se conoce como la Google Hacking Database, en la cual se encuentran almacenados cientos de términos de búsqueda y también es autor del libro “Google

Hacking for penetration testers", donde describe las técnicas de búsqueda avanzada, junto a mecanismos para automatizarlas.

Como se comentó anteriormente, Google ofrece lo que se denomina operadores avanzados para potenciar las búsquedas. Cuando los operadores avanzados no se utilizan en una consulta, Google localiza los términos de búsqueda en cualquier área de un sitio web, incluyendo el título de páginas, el contenido, la URL, entre otros. Cuando son utilizados correctamente, estos operadores pueden ayudar a obtener exactamente la información que se está buscando, sin tener que gastar demasiado tiempo estudiando detenidamente el sitio web del objetivo. Algunos de los operadores pueden ser combinados con otros, pero existen algunos que no permiten ser combinados.

Los operadores avanzados no son más que una parte de una consulta, pero tienen una sintaxis bastante rígida que se debe seguir. La sintaxis básica de un operador avanzado de Google es: *operador:Termino-de-búsqueda*. Al utilizar operadores de búsqueda avanzados, hay que tener en cuenta lo siguiente:

- No hay espacio entre el operador, los dos puntos, y el término de búsqueda.
- Los términos de búsqueda siguen la misma sintaxis que los términos de búsqueda simples. Por ejemplo, se puede proporcionar un término de búsqueda como una sola palabra o una frase entre comillas. Si se proporciona una frase como término de búsqueda, debe asegurarse de que no hay espacios entre el operador, los dos puntos, y la primera cita de la frase.
- Operadores booleanos y caracteres especiales pueden ser utilizados en los términos de búsqueda.
- Los operadores avanzados pueden ser combinadas en una sola consulta, siempre y cuando se respete la sintaxis básica, así como la sintaxis particular de operador. Hay que tener en cuenta que existen algunos operadores avanzados que simplemente no se pueden combinar (los denominados ALL).

En la Tabla 1, se pueden ver algunos operadores frecuentemente utilizados:

Tabla 1. Operadores avanzados combinables de Google Hacking.

Operador	Descripción	Argumentos
site	Limita la búsqueda a un determinado dominio	El dominio específico
inurl	Busca una palabra en las URL de las páginas web	Una palabra o una expresión entre comillas

Operador	Descripción	Argumentos
intitle	Busca una palabra específica en el título de las páginas web	Una palabra o una expresión entre comillas
intext	Busca una palabra en el texto de las páginas web	Una palabra o una expresión entre comillas
filetype	Busca archivos con determinada extensión	Extensiones de archivos a buscar
inanchor	Busca palabras presentes en la descripción de los enlaces	Una palabra o una expresión entre comillas

Fuente: elaboración propia.

Navegación Anónima

Claro está que un atacante tratará siempre de permanecer anónimo y levantar la mínima cantidad de sospechas. Para un analista de seguridad la realidad es diferente, dependiendo del tipo de análisis que se esté llevando adelante, abierto/encubierto, puede ser útil realizar el reconocimiento de manera anónima o no.

Antes de comenzar se describirá, en términos genéricos, lo que se denomina servidor proxy para efectos de comprender su función. Se puede decir que, un servidor proxy es un intermediario entre el sistema del usuario y el servicio de Internet al cual se quiere acceder. En particular, un proxy web es un intermediario entre el navegador del usuario y el servidor web que se consulta, habitualmente un servidor web en Internet. Puede servir como filtros de contenido, bloqueando el acceso a determinados sitios. También son utilizados para mejorar el rendimiento, ya que pueden guardar, durante cierto tiempo en memoria caché, las páginas web a las que se acceden. Cuando se solicita la misma página web, el servidor proxy utiliza la información guardada en el caché en lugar de recuperarla del proveedor.

Un detalle importante es que un equipo detrás de un proxy es completamente oculto, y su dirección IP no se revela. De alguna manera, la navegación se transforma en anónima o indirecta.

El Traductor de Google: una forma de obtener información de un sitio en forma anónima es utilizar el traductor de Google. Esta técnica requiere únicamente de la dirección URL del objetivo, lo que hay que hacer es generar una traducción de dicha dirección a través del servicio de traducción de Google.

Actualmente Google no permite utilizar el truco que consiste en realizar una traducción de un idioma a sí mismo (inglés a inglés, o español a español, por ejemplo), pero si traducimos a otro idioma, Google nos muestra la información en

el idioma original y la traducción. Está técnica también permite obtener información sin realizar consultas directas al servidor objetivo.

Servidores proxy públicos: lo anterior no es la forma más efectiva, ya que existen en Internet servidores proxy públicos. Detrás de este tipo de servidores, la dirección IP será invisible a todos los sitios web que se consulten. Como cualquier tecnología también puede ser utilizada para mal, los atacantes pueden esconderse detrás del proxy para originar ataques, y la dirección que quedará registrada en la víctima es la del servidor proxy.

De todas maneras, para bien o para mal, el propio proxy tiene información sobre su uso. En caso de ser necesario, dependiendo de la legislación de cada país, si se causan daños en algún servidor de Internet desde la IP del proxy, las autoridades podrían consultar los registros del servidor proxy y detener al atacante. En el siguiente enlace se pueden encontrar una lista de servidores proxy anónimos https://www.proxynova.com/proxy-server-list/

Servidores proxy en cadena: una técnica, para evitar el inconveniente anterior, es la llamada proxy en cadena (también conocida como daisy-chain). Es una sucesión de enlaces tal que un dispositivo A es conectado a un dispositivo B, el mismo dispositivo B a un dispositivo C, este dispositivo C a un dispositivo D, y así sucesivamente. Entre cada uno de estos dispositivos se utiliza un proxy. El aumento del número de intermediarios agrega una dificultad adicional para los investigadores, que deben analizar los registros de cada uno de ellos.

Utilizar servidores proxy públicos para atacar un objetivo requiere de muchos cuidados, incluso para los atacantes más experimentados, por esta razón, otra de las maneras para no ser descubiertos es buscar servidores proxy mal configurados y utilizarlos para dichos propósitos.

Red TOR: en el contexto de tratar de lograr anonimato, uno de los proyectos a destacar es TOR (The Onion Router). Es una implementación libre de un sistema de ruteo llamado enrutamiento cebolla que permite a sus usuarios comunicarse en Internet de manera anónima. TOR es una red de túneles virtuales que permiten a personas y grupos mejorar su privacidad y seguridad en Internet. Proporciona la base para una serie de aplicaciones que permiten a las organizaciones y personas compartir información mediante el uso de redes públicas sin comprometer su privacidad. Más información sobre este proyecto y sus funcionalidades se puede encontrar en: https://www.torproject.org/.

Análisis de metadatos de archivos: el término metadatos no tiene una definición única y literalmente hace referencia a los "datos sobre otros datos". Sin lugar a duda, esto no dice mucho acerca de su posible aporte, más concretamente se puede decir que es un concepto utilizado esencialmente para designar conocimiento asociado a determinado objeto o recurso. Es decir, información descriptiva que se estructura de tal forma que permite ayudar en la identificación, descripción, clasificación y administración de instancias de evaluación.

Cuando se hace referencia a objetos digitales, se denomina metadatos a la información que es insertada en los archivos por el software de edición o creación de estos. Contienen información acerca de la creación del archivo como: nombre de autor, autores anteriores, nombre/modelo del dispositivo que lo origina, cantidad de veces que fue modificado, fecha de creación, entre otros.

Los metadatos facilitan el flujo de trabajo, por ejemplo, convirtiendo datos automáticamente de un formato a otro. Sin embargo, también suponen un riesgo, especialmente por lo poco que se los tiene en cuenta, y son potencialmente peligrosos por la cantidad de información sensible que contienen, siendo ésta de gran utilidad para potenciales atacantes.

En general, se tiende a pensar en los metadatos agregados a los documentos por las herramientas de Ofimática, pero no son los únicos. A modo de ejemplo, se puede nombrar a ID3 (Iterative Dichotomiser 3) que es un estándar de facto para incluir metadatos en un archivo audiovisual, se utiliza principalmente en archivos sonoros como MP3. También se puede nombrar a EXIF (Exchangeable image file format), es una especificación para formatos de archivos de imagen usado por las cámaras digitales.

Los datos de un objeto de evaluación se pueden obtener en una variedad de maneras, aplicando diferentes técnicas de revisión. Estas técnicas se caracterizan por examinar en forma pasiva instancias de evaluación. Las consultas en Google, WHOIS, DNS y el análisis de metadatos juegan un papel preponderante.

El proceso implica comenzar con información general y aplicando una metodología iterativa se reconstruyen detalles específicos a partir de la información que se va obteniendo. Algunos de los objetivos pueden ser: determinar los nombres de dominio utilizados, usuarios de los sistemas, información detallada sobre las máquinas y dispositivos de una red y todo aquello que nos permita generar una estrategia para las etapas sucesivas. Un detalle importante es que ninguna pieza de datos debe ser

pasada por alto durante una evaluación, sobre todo cuando se trata de un objetivo bien asegurado.

Vale la pena destacar que, si bien las técnicas expuestas están basadas en métodos tecnológicos, esencialmente basados en búsquedas en Internet, cualquier otro tipo de fuente puede ser útil. A modo de ejemplo, algunos métodos no técnicos son: consultar folletos de la empresa con los servicios que brinda, anuncios en periódicos y documentos internos.

Si bien la información se expone con fines legítimos, puede ser utilizada con otras intenciones. Contratar a expertos para realizar tareas de reconocimiento es una actitud diligente que puede ayudar a mitigar problemas. Como se vio, todas las técnicas descritas pueden ser utilizadas a través de canales anónimos o no, dependiendo de si el análisis es abierto o encubierto.

5.3.2. Descubrimiento

En este punto, un atacante cuenta con información táctica, tiene más certezas y conocimiento de su objetivo. A modo de ejemplo, puede conocer cuál es el modelo de negocios subyacente en la organización; hacerse una idea del impacto que podría causar una fuga de información y cuál es el valor que ésta podría tener; cuáles son las identidades de las personas, técnicas y no técnicas, involucradas. Es decir, todo aquello que la etapa de reconocimiento le pudiera brindar.

El atacante se encuentra en una posición en la cual podría ser capaz de establecer un propósito específico y elaborar planes estratégicos. Si bien la motivación y el propósito pueden venir establecidos desde la etapa de reconocimiento, dependiendo de la información de contexto obtenida, estos pueden cambiar. Pueden pasar de simplemente molestar a su víctima a obtener algún rédito económico. Un analista de seguridad debe de ser capaz de identificar los posibles propósitos de un atacante. Consecuentemente, y tal cual lo hace un atacante, necesita identificar los blancos de ataque y descubrir brechas de seguridad, para evaluar que tan expuestos se encuentran los activos de la organización en cuestión.

En general, en esta etapa se utilizan métodos de acceso directos a los objetivos, donde se establecerá algún tipo de interacción o contacto con ellos, y de esta manera se efectuarán diferentes pruebas para encontrar información adicional.

Siguiendo con la analogía del delincuente, después de que el mismo cuente con la información de contexto necesaria, podría decidir obtener más información realizando acciones que involucren alguna interacción con su víctima. Por ejemplo,

suponemos que de la etapa de reconocimiento ya sabe los horarios de los residentes, si se tiene una cerca, un perro, barras en las ventanas y puertas. Ahora, en la etapa de identificación y descubrimiento, necesita validar algunas hipótesis y decide ir hasta la casa e intentar ver a través de las ventanas y romper vidrios para corroborar la presencia de alarmas y tiempos de respuesta de los servicios de seguridad.

El descubrimiento tiene como cometido encontrar elementos que son desconocidos, estos elementos pueden, entre otros, ser: dispositivos, puertos TCP/UDP abiertos, información disponible, entre otros. De esta manera se comenzará a recopilar datos sobre los objetos de evaluación y el propósito de estos.

Es común que los tiempos en una evaluación de seguridad sean limitados, consecuentemente, los pasos deben ser racionalizados para que el tiempo rinda y sea productivo. Dicho de otra manera, se busca solamente analizar los puertos en dispositivos que aparentan estar activos. Es aquí donde la información recopilada en la etapa de reconocimiento comienza a cobrar importancia.

Dependiendo del tipo de análisis los objetos de evaluación pueden haber sido fijado de antemano. La organización puede solicitar un servicio sobre determinado conjunto de red o dispositivo, por ejemplo, puede dar un rango de direcciones IP o una única dirección que corresponde con un dispositivo. En esta línea, y si no se encuentran establecidos de antemano los objetos de evaluación, una lista potencial es la obtenida en la fase de reconocimiento. A modo de ejemplo, hay que recordar que en la fase de reconocimiento se realizan consultas o transferencias de zonas DNS. Si un nombre es asignado a una dirección IP, posiblemente dicha dirección corresponda a un dispositivo activo. Esto no quiere decir que no se pueda apuntar a cualquier dispositivo dentro de los rangos establecidos, pero puede que se pierda tiempo tratando de analizar un sistema que tal vez no exista, o no sea accesible desde la ubicación que se encuentra el analista. En este sentido, en base a la información que se disponga se puede establecer una lista de prioridades, comenzado a trabajar con los objetivos potencialmente activos dentro del rango y dejar para el final aquellos de los que no se cuente con información. Por otro lado, también tenemos el concepto la Identificación, el cual es el proceso que permite enumerar y reconocer la identidad de los servicios y recursos específicos que ofrece determinado objeto de evaluación. Se puede efectuar la identificación comenzando con un conjunto de parámetros, como ser un conjunto de direcciones IP activas y los puertos abiertos en el sistema (provenientes del descubrimiento). Términos como captura de banners y finger printing son utilizados en este contexto.

Es de suponer que la información de posibles objetivos, obtenida en la fase de reconocimiento, no necesariamente es completa y fidedigna. Consecuentemente, es necesario comenzar a depurar y validar las hipótesis de trabajo. Es razonable entonces, comenzar por determinar los sistemas activos y su capacidad de respuesta.

El proceso para llevar a cabo en la fase de descubrimiento incluye:

- *Escaneo de puertos*: Una vez que se identifican los dispositivos activos, se procede a identificar el tipo de dispositivo, estado de los puertos, servicios brindados y el sistema operativo instalado.
- *Identificación de Servicios:* luego de identificar el estado de los puertos, es necesario averiguar qué es lo que se está ejecutando en dichos puertos.
- *Detección de sistemas operativos:* Obtener la versión del sistema operativo puede ser un paso muy valioso en la etapa de identificación y descubrimiento, ya que puede sesgar las decisiones de un atacante y marcar pautas para el analista de seguridad.

Más allá de la potencial trascendencia que esta fase pueda llegar a tener, en un proceso de evaluación de seguridad hay ciertos límites explícitos que son acordados entre las partes durante el proceso de planificación. Dependiendo de la amplitud y el alcance, es posible que el analista de seguridad se encuentre limitado a examinar determinado rango o tipo de objetivo o puede ser libre de inspeccionar todo lo que se encuentre a su alcance, esto lo haría un poco más interesante.

En todos los casos, es necesario asegurarse de:

- Sólo se realizarán pruebas sobre los objetivos oportunamente aprobados.
- Buscar toda la información posible antes de aumentar la profundidad de los ataques.
- Identificar cada tipo de objetivo y su finalidad dentro de la organización, es decir, qué servicios ofrece.
- Obtener información específica acerca de las versiones y tipos de servicios que se ejecutan en los sistemas.
- Tomar las precauciones necesarias para no dejar fuera de servicio un activo crítico de la organización.

Al momento de realizar las tareas de campo hay que tener en cuenta que un proceso de descubrimiento mal diseñado, con un sondeo simplista, disminuye la eficiencia de

las pruebas. Mientras que, por otro lado, generar tráfico extra e innecesario puede ser contraproducente para el análisis y la organización. Es ineficaz analizar un servicio con un método diseñado para otro, lo que en ciertas situaciones puede generar una denegación de servicios (DoS). Generar un DoS no es una buena idea, a menos que haya sido específicamente encargado como parte del alance del trabajo a realizar.

5.3.2.1. Técnicas y herramientas

Existen técnicas pasivas y activas para detectar dispositivos activos en una red, teniendo cada una de ellas sus ventajas y desventajas. Dentro de las técnicas activas, las más comunes se basan en la utilización del protocolo Internet Control Message Protocol (ICMP). ICMP es el protocolo utilizado por el comando Ping y muchas veces, para evitar diferentes tipos de ataques como DoS o ping flood, se bloquea este tipo de peticiones en una red. De todas maneras, en un análisis de seguridad no hay que desestimar ninguna prueba, es necesario evaluar las respuestas de este tipo de peticiones y verificarlas, dependiendo de la posición que se encuentre el analista. Si los paquetes ICMP son bloqueados se pueden utilizar paquetes TCP ACK. Es común que en la bibliografía a esta técnica se la denomine ping TCP. El RFC 1122 indica que las repuestas a los paquetes ACK no solicitado deben devolver un paquete TCP RST. Por lo tanto, el envío de este tipo de paquetes a un puerto accesible, por ejemplo, a través de un muro de fuego (firewall), debe responder con un RST, siendo esto indicación de que el objetivo está activo (Hernández, 2014).

Por otro lado, también existe lo que se denomina ping UDP, la idea es enviar un paquete UDP vacío a determinado puerto UDP. Si el dispositivo se encuentra activo y el puerto en cuestión está cerrado, se debería generar un paquete ICMP (Port Unreachable). Consecuentemente, si se obtiene una respuesta, se puede identificar que el objetivo se encuentra activo y alcanzable por el ping UDP.

La desventaja del ping UDP es que si en el puerto al que se le manda el paquete se encuentra atendiendo un servicio simplemente se descartará el paquete vacío y no se devolverá ninguna respuesta. Por esta razón se utilizan puertos que no son estándar para enviar este tipo de paquetes, ya que es altamente probable que dicho puerto no se encuentre utilizado por un servicio.

En un análisis de seguridad, dentro de las técnicas de descubrimiento activas se busca combinar los métodos ping ICMP, TCP y UPD. La finalidad de este tipo de pruebas es intentar pasar a través de dispositivos de seguridad, por ejemplo, firewalls o filtros que sólo analizan alguno de los tres protocolos y descuidan otros. Algunas herramientas que trabajan técnicas activas son:

Tabla 2. Herramientas de reconocimiento activo.

Nombre de la herramienta	Características
Nmap	Es una aplicación multiplataforma usada para explorar redes y obtener información acerca de los servicios y sistemas operativos de hosts en una red.
Hping3	Es una herramienta que se utiliza desde la consola o terminal en Linux, cuyo fin es el análisis y ensamblado de paquetes TCP/IP
Xprobe2	Es básicamente una herramienta activa OS Fingerprinting que envía datos reales a la máquina objetivo.
Unicornscan	Es un nuevo motor para la captura y correlación de información, construido para y por los miembros de las comunidades de investigación y pruebas de seguridad.

Fuente: elaboración propia.

Si el analista se encuentra dentro de la red, las técnicas de descubrimiento pasivas pueden ser otra opción o un complemento a las activas. En el escenario activo, el objetivo responde a los estímulos proporcionados por una herramienta, básicamente es una condición de observación artificial que se crea para evaluar las respuestas. En el escenario pasivo, el objetivo responde a los estímulos derivados de su uso normal y la herramienta solamente observa dicha comunicación. En ambos casos se pueden ver los puertos y los servicios involucrados, el flujo de la conexión, la información de tiempo, entre otros. De esta manera, a partir de los datos resultantes se pueden hacer algunas conjeturas sobre las características de funcionamiento de la red.

La técnica pasiva permite algo (además de no generar tráfico) que la activa no: se puede observar la red desde la perspectiva del comportamiento de las aplicaciones durante las operaciones normales, sin generar alarmas, por ejemplo, en los IDS o entradas en las bitácoras de los dispositivos involucrados.

Ubicar los dispositivos de descubrimiento pasivo no es una tarea trivial, pues tienen que situarse en lugares que les permita ver el tráfico de interés, hoy en día dadas las posibilidades que brindan los concentradores (switches) y las redes virtuales (VLAN), es una tarea compleja.

Algunos de los usos potenciales de las técnicas pasivas son:

- *Toma de conciencia:* estas técnicas de análisis pueden decir mucho acerca de la red en cuestión y la forma en que funciona normalmente.

- *Aplicación de políticas*: puede ayudar a identificar servicios ilegales y mal comportamiento de los usuarios de la red.
- *Detección de amenazas internas*: el análisis pasivo tiene el potencial de ayudar a identificar equipos comprometidos, que no se detectan desde una vista perimetral.

Ejemplos de herramientas a utilizar son: autoscan, ettercap, networkminer y wireshark. El resultado, tanto de los barridos y las técnicas pasivas, es una lista de dispositivos activos que se utilizará como insumo para lo que se denomina escaneo de puertos.

Tabla 3. Herramientas de reconocimiento pasivo.

Nombre de la herramienta	Características
Autoscan	Es un escáner de red que permite explorar y controlar los dispositivos y equipos conectados en ella.
Ettercap	Es un interceptor/sniffer para redes de área local con switch. Soporta direcciones activas y pasivas de varios protocolos (incluso aquellos cifrados, como SSH y HTTPS).
Networkminer	Es un analizador de paquetes y protocolos muy utilizado para ayudarnos a detectar desde problemas en nuestras redes (por ejemplo, problemas con algún equipo que esté saturando la red) hasta la más mínima fuga de datos (contraseñas, datos personales sin cifrar, etc).
Wireshark	Es un analizador de protocolos utilizado ampliamente para realizar análisis y solucionar problemas en redes de comunicaciones, para desarrollo de software y protocolos. Es una gran herramienta para gestión de redes.

Fuente: elaboración propia.

5.3.3. Escaneo de puertos

Se entiende como puerto a la interfaz lógica que permite enviar y recibir información entre dos o más equipos conectados en red. Tradicionalmente los estados de los puertos se dividen en dos: abierto o cerrado. Un puerto abierto indica que una aplicación acepta conexiones TCP o paquetes UDP en dicho puerto identificado por números comprendidos entre 1 y 65535. Debido a que son vectores de ataques, encontrar puertos abiertos es generalmente el objetivo primario de un atacante.

Un puerto cerrado es accesible, recibe y responde a las conexiones, pero no tiene una aplicación escuchando en él. Son útiles para determinar si un equipo está activo en cierta dirección IP. Según la herramienta utilizada se puede tener otra clasificación, en particular NMAP clasifica los puertos en seis estados: abierto, cerrado, filtrado, no filtrado, abierto/filtrado o cerrado/filtrado.

En términos generales, en lo que refiere al escaneo de puertos, se puede decir que todas las herramientas en esencia funcionan de manera similar. El comportamiento típico es: enviar un paquete, analizar la respuesta y formular algún tipo de conclusión sobre el estado del sistema o el puerto.

Repasando el funcionamiento del protocolo TCP y según el RFC793, en particular estudiando las banderas de control, tenemos que existen las siguientes banderas que todo analista de seguridad debe conocer:

- SYN se utiliza para establecer una conexión TCP, para sincronizar los números de secuencia entre ambos extremos.
- ACK sirve para confirmar al emisor que la recepción de su paquete fue satisfactoria.
- RST al enviar un paquete con esta bandera activada, se indica que hubo problemas de conexiones y que será necesario reiniciar la conexión para sincronizar ambas partes nuevamente.
- FIN indica al host remoto que se quiere cerrar la conexión, y se queda a la espera de la respuesta.
- URG significa que el paquete que se envía contiene datos de URGENCIA. Esto quiere decir que un paquete con bandera URG tendrá privilegio ante otros datos del paquete y se leerá primero.
- PUSH quiere decir que se debería vaciar el buffer de transmisión, cuando se envía información grande se divide en paquetes, estos se sitúan en un buffer de transmisión.

Las técnicas de identificación y descubrimiento basan su operación en efectuar acciones que no estén estrictamente prohibidas dentro de los RFC. En esta línea, se pueden realizar intentos de conexión a los diferentes puertos y en caso de obtener una respuesta establecer dicha conexión. La desventaja de este enfoque es que deja información en las bitácoras de los dispositivos involucrados. Otra línea de acción es crear paquetes con malformaciones que permitan explotar debilidades de seguridad intrínsecas a los protocolos. Un paquete mal formado es un paquete de cualquier

tipo de protocolo de comunicación, con parámetros diferentes a los que se han establecido en su RFC. A modo de ejemplo, en el caso particular de TCP se pueden alterar las banderas de control. Esto es permitido, debido a que se asume que los protocolos de comunicación se establecieron como las normas de operación entre dos o más dispositivos de comunicación en un canal que puede introducir errores y malformaciones.

Dentro de los tipos básicos de análisis de puertos TCP, el más común es un sondeo SYN, llamado así por el uso de la bandera de control TCP SYN que aparece en la secuencia de inicio de conexión TCP (handshake). Este tipo de exploración se inicia mediante el envío de un paquete SYN a un puerto de destino. El destino recibe el paquete SYN, responde con un SYN/ACK de respuesta si el puerto está abierto o un RST si el puerto está cerrado. El sondeo SYN es relativamente rápido y cauteloso ya que no se llega a completar el handshake de inicio de conexión y posiblemente no quede registrado en las bitácoras. Otros tipos de escaneo de puertos pueden utilizarse para situaciones específicas, en ellos se emplean diversas banderas TCP, como FIN, PUSH, y URG (Hernández, 2014).

Para obtener conclusiones interesantes y claras hay que poner mucha atención a los resultados o respuestas sea:

1. Un paquete con la bandera de ACK activa a un puerto cualquiera, esté abierto o cerrado, deberá ser respondido con un RST.
2. Un paquete con la bandera de FIN activa deberá ser respondido con RST & ACK ante un intento a un puerto cerrado y nada ante un intento en un puerto abierto.
3. TCP sin banderas activas, el destino deberá responder con un paquete con RST & ACK activas si el puerto estaba cerrado y nada si está abierto.

Aunque el protocolo UDP no está orientado a conexión, es posible realizar un escaneo y en el caso de los puertos UDP cerrados, estos deben responder ante una petición de conexión, lo que puede ser explotable por un posible atacante. Si se envía un paquete a un puerto que no está abierto, responde con un mensaje ICMP (Port Unreachable). Consecuentemente, se infiere que si no hay respuesta el puerto está abierto. Claramente, en caso de que un firewall filtre las respuestas pueden generarse muchos falsos positivos. Es pertinente aclarar que este método es afectado por las recomendaciones del RFC 1812, más específicamente la sección 4.3.2.8, que refiere al Rate Limiting, que hacen que este tipo de escaneo se vuelva muy lento.

El protocolo UDP no proporciona fiabilidad, por lo que será necesario retransmitir los paquetes para tener ciertas garantías de que llegan a su destino. Por dicha razón, otra técnica es enviar paquetes UDP a puertos estándar y operar con protocolos de capas superiores, por ejemplo, enviar una consulta DNS o SNMP.

Al igual que los pings en línea, existen en Internet sitios que ofrecen servicios de escaneo de puertos en línea. En general, permiten chequear una lista predeterminada de puertos bajo algunos "términos de uso" y limitaciones. Este tipo de herramientas permiten un primer acercamiento indirecto mediante el cual se obtiene información con cierto grado de anonimato.

A continuación, algunos puertos conocidos:

Tabla 4. Puertos y protocolos comúnmente conocidos.

Puerto/ protocolo	Nombre	Descripción
11/tcp	systat	Servicio del sistema para listar los puertos conectados
13/tcp	daytime	Protocolo Daytime, envía la fecha y hora actuales
17/tcp	qotd	Quote of the Day, envía la cita del día
18/tcp	msp	Protocolo de envío de mensajes
19/tcp	chargen	Protocolo Chargen o Generador de caracteres, envía flujos infinitos de caracteres
20/tcp	ftp-data	FTP File Transfer Protocol (Protocolo de Transferencia de Ficheros)- datos
21/tcp	ftp	FTP File Transfer Protocol (Protocolo de Transferencia de Ficheros)- control
22/tcp	ssh	SSH, scp, SFTP
23/tcp	telnet	Telnet manejo remoto de equipo, inseguro
25/tcp	smtp	SMTP Simple Mail Transfer Protocol (Protocolo Simple de Transferencia de Correo)
37/tcp	time	Time Protocol. Sincroniza hora y fecha
39/tcp	rlp	Protocolo de ubicación de recursos
42/tcp	nameserver	Servicio de nombres de Internet
43/tcp	nickname	Servicio de directorio WHOIS
49/tcp	tacacs	Terminal Access Controller Access Control System para el acceso y autenticación basado en TCP/IP
50/tcp	re-mail-ck	Protocolo de verificación de correo remoto
53/tcp y udp	domain	DNS Domain Name System (Sistema de Nombres de Dominio), por ejemplo BIND se ejecuta en ese puerto.
63/tcp	whois++	Servicios extendidos de WHOIS (WHOIS++)
66/tcp and udp	Oracle SQLNet	Software de red que permite acceso remoto entre los programas y la base de datos Oracle.

Puerto/ protocolo	Nombre	Descripción
67/udp	bootps	BOOTP BootStrap Protocol (servidor), también usado por DHCP.
68/udp	bootpc	BOOTP BootStrap Protocol (cliente), también usado por DHCP.
69/udp	tftp	TFTP Trivial File Transfer Protocol (Protocolo Trivial de Transferencia de Ficheros)
70/tcp	gopher	Es un servicio de Internet consistente en el acceso a la información a través de menús.
79/tcp	finger	Proporciona información de los usuarios de una máquina, estén o no conectados en el momento de acceder al servicio
80/tcp	http	HTTP HyperText Transfer Protocol (Protocolo de Transferencia de HiperTexto) (WWW)
88/tcp	kerberos	Kerberos Agente de autenticación
110/tcp	pop3	POP3 Post Office Protocol (E-mail)
115/tcp	sftp	SFTP Protocolo de transferencia de archivos seguros
119/tcp	nntp	NNTP usado en los grupos de noticias de usenet
123/udp	ntp	NTP Protocolo de sincronización de tiempo
143/tcp	imap	IMAP4 Internet Message Access Protocol (E-mail)
161/udp	snmp	SNMP Simple Network Management Protocol
162/udp	snmptrap	SNMP-trap
179/tcp	bgp	Border Gateway Protocol
220/tcp	imap3	IMAP versión 3
245/tcp	link	Servicio LINK / 3-DNS iQuery
443/tcp	https	HTTPS/SSL usado para la transferencia segura de páginas web
445/tcp	microsoft-ds	Microsoft-DS (Active Directory, compartición en Windows, gusano Sasser, Agobot) o también es usado por Microsoft-DS compartición de ficheros
465/tcp	smtps	SMTP Sobre SSL. Utilizado para el envío de correo electrónico (E-mail)
514/udp		syslog usado para logs del sistema
515/tcp		usado para la impresión en windows
521/udp	ripng	RIP Routing Information Protocol IPv6 (Protocolo de Información de Enrutamiento Internet v6)2
587/tcp	smtp	SMTP Sobre TLS
690/tcp		VATP (Velneo Application Transfer Protocol) Protocolo de comunicaciones de Velneo
993/tcp	imaps	IMAP4 sobre SSL (E-mail)
995/tcp		POP3 sobre SSL (E-mail)

Fuente: elaboración propia.

5.3.4. Escaneo de servicios

El escaneo de puertos se basa en la capacidad de recopilar información de un puerto TCP/UDP abierto, ya sea en forma directa, mediante el establecimiento de una conexión o por inferencia a partir de la construcción de paquetes con malformaciones.

El resultado de un escaneo de puertos es una lista de direcciones IP donde a cada dirección le corresponde un conjunto de puertos abiertos. Luego de que se identificó el estado de los puertos y se tiene como resultado la lista mencionada anteriormente, es necesario averiguar y verificar lo que se está ejecutando en dichos puertos.

Normalmente se conoce que SMTP se ejecuta en el puerto TCP/25, pero si el administrador del sistema está tratando de confundir a los posibles atacantes, puede ejecutar otra aplicación en su lugar. La forma más sencilla de comprobar lo que se encuentra detrás de un puerto abierto es capturar los "banners" asociados.

En las instalaciones predeterminadas y al momento de atender una petición las aplicaciones con salida ASCII despliegan un banner (también conocido como anuncio). El procedimiento consiste en conectarse al servicio, capturar la respuesta y compararla con una lista de respuestas conocidas. Debido a la facilidad con la cual se puede modificar el banner de un servicio, el uso de esta técnica es limitada y puede conllevar a generar falsos positivos. De todas maneras, en un análisis de seguridad se debe de tener en cuenta este procedimiento, combinándolo con otro tipo de técnicas para validar y verificar los resultados.

Un método alternativo para obtener información de servicios y sistemas operativos sin hacer ningún tipo de consulta directa es utilizar servicios como los ofrecidos por NETCRAFT (http://www.netcraft.com). NETCRAFT es una compañía dedicada, básicamente, a realizar estadísticas del uso de software en Internet. Esta compañía dispone de un servicio Web donde al introducir el nombre del dominio proporciona información acerca del mismo, el sistema operativo, entre otros datos de interés.

5.3.5. Detección de sistemas operativos

Es muy posible que, según la versión del sistema operativo, las búsquedas en Internet revelen vulnerabilidades y debilidades propias del sistema en cuestión. Una vez que el atacante conoce dicha versión puede recopilar datos para ataques específicos o utilizar los datos como una herramienta en un ataque de ingeniería social. Identificar un sistema operativo puede implicar la realización de tareas con diferentes niveles de complejidad, desde simplemente forzar al sistema a mostrar un banner a tener que utilizar herramientas para realizar consultas TCP específicas.

En general se combinan una cantidad suficiente de elementos para tratar de identificar, con un alto grado de precisión, el sistema subyacente. Se utiliza el término "OS fingerprint" para denominar el proceso de detección de sistemas operativos o como se indicó en secciones anteriores de este documento, firma de sistemas operativos. El objetivo de estas firmas es determinar el tipo y la versión del sistema operativo subyacente. Los métodos de exploración se dividen en activos y pasivos. Los métodos activos analizan las respuestas obtenidas del envío paquetes TCP, UDP o ICMP. El proceso, utilizando paquetes TCP, consiste en fijar distintas banderas de control y observar las respuestas, éstas difieren dependiendo del sistema operativo (SO) y también entre diferentes versiones de un mismo SO. Por lo general se envían varios paquetes TCP y las respuestas son comparadas con bases de referencia conocidas, bases de huellas dactilares o OS fingerprint. Usualmente los métodos basados en ICMP utilizan menos paquetes que los métodos basados en TCP, por lo tanto, cuando es necesario ser cauteloso puede ser buena práctica utilizar ICMP, aunque hay que tener en cuenta que el mecanismo es menos preciso. La identificación pasiva se caracteriza por utilizar herramientas tipo analizador de protocolos s o husmeadores que pasivamente recogen paquetes. Luego, dichos paquetes serán analizados y al igual que en las técnicas activas serán comparados con una base de referencia. Esto, obviamente, tiene una funcionalidad limitada. Puede, sin embargo, ser útil si el analista de seguridad se encuentra en el mismo dominio de colisión de paquetes que los objetivos a analizar. Una técnica indirecta para detectar el sistema operativo es consultar los puertos y servicios que ofrece el dispositivo. Es de público conocimiento que hay aplicaciones que solamente pueden ser ejecutadas sobre determinado SO, al igual que determinados puertos están abiertos en uno u otro SO.

El tiempo de retransmisión en TCP también puede ser una técnica utilizada para identificar el sistema operativo. TCP está diseñado para ser orientado a conexión, para hacer cumplir las normas de diseño una conexión debe ser solicitada y reconocida antes de que cualquier transferencia pueda tener lugar, y cada paquete debe ser reconocido y aceptado exitosamente. Si un paquete no se recibe en un período predeterminado de tiempo debe ser reenviado. El RFC 793 no define explícitamente un algoritmo para determinar el momento de volver a enviar un paquete perdido, consecuentemente cada sistema operativo toma su decisión y de esta manera se puede obtener un fingerprint de cada sistema operativo.

5.3.5.1. Técnicas y herramientas

A continuación, se mostrarán algunas herramientas que se pueden utilizar en esta fase sin pretender ser exhaustivos ni explicar todas las formas de usar cada una de las ellas. Simplemente y a modo de ejemplo, se verán algunas opciones que se corresponden con el proceso descripto en este capítulo. Por más información se debe recurrir al manual oficial de cada herramienta. Se hace especial énfasis en la herramienta NMAP, ya que al ser la misma de multipropósito abarca varios de los puntos explicados en esta sección.

Nmap Security Scanner: en general, las herramientas que se dedican a escanear puertos aceptan como entrada una dirección IP de destino o un rango de red. Mediante diferentes técnicas detectan los dispositivos activos y luego envían una consulta a determinados puertos. Como salida, crean una lista que contiene las respuestas de cada puerto.

El escáner más popular es Nmap Security Scanner, escrito por Gordon Lyon, conocido en Internet como Fyodor. La herramienta se encuentra disponible en el sitio www.insecure.org.

Como se mencionó anteriormente Nmap es una herramienta multipropósito y se ha convertido en un estándar por defecto en las evaluaciones de seguridad.

A continuación, se repasarán algunas de las funcionalidades más utilizadas.

1. Detección de dispositivos: antes de escanear los puertos es necesario determinar los dispositivos activos, es decir realizar la etapa de descubrimiento. Para ello se puede considerar la funcionalidad de barrido de Nmap, también conocida como el ping de Nmap. Para determinar si un equipo está activo, se activará la funcionalidad con la opción -sP y cuando se invoca como root, enviará paquetes ICMP Echo Request y paquetes TCP SYN. Ejemplo: Nmap-sP ip_address. Sin embargo, si de antemano se sabe que los paquetes ICMP están bloqueados y no se desea enviar dichos paquetes, alcanza con modificar el tipo de ping Nmap con la opción-P. Por ejemplo, al invocar con-P0-PS solamente se utiliza el método de exploración denominado ping TCP. Con-P0 se indica "NO ping ICMP" y "PS indica" el uso del método TCP SYN. Un detalle para tener en cuenta es que al utilizar una sola variante de exploración se incrementa la velocidad de ejecución de la herramienta. Usar múltiples métodos puede no ser un gran problema cuando se escanean pocos sistemas, pero es un punto para considerar cuando se escanean rangos de direcciones IP muy grandes. También es importante remarcar que si Nmap no puede ver el objetivo no lo

analizará, a menos que la opción-P0 (no ping) se utilice. Hay que ser cuidados, pues el uso de la opción-P0 puede crear problemas, ya que Nmap analizará cada uno de los puertos del destino, incluso si el objetivo no está activo. Para lograr un buen equilibrio se debe considerar el uso de la opción-P para seleccionar otro tipo de comportamiento de ping. Por ejemplo, la opción del -PP usará paquetes ICMP Timestamp requests y la-PM opción utilizará ICMP Netmask requests. Antes de realizar un barrido completo sobre un rango de direcciones IP (una red), puede ser de ayuda utilizar la información de la etapa de reconocimiento. De esta manera se pueden realizar pruebas sobre algunas direcciones IP conocidas, tales como servidores web, servidores DNS, servidores de correo electrónico y así sucesivamente, buscando optimizar y reducir el número total de paquetes enviados y el tiempo necesario para el análisis.

2. Escaneo de puertos: Nmap brinda muchos mecanismos para realizar un escaneo de puertos. De todos los mécanismos posibles, no es una buena idea utilizar lo que se denomina connect scan (-sT). Connect scan es un método que establece una conexión TCP completa a un puerto. Hay que tener en cuenta, que estableces muchas conexiones TCP puede causar una denegación de servicio y/o activar las alarmas de los IDS's de la organización. Lo fundamental es utilizar un método de escaneo de puertos “sigiloso”, uno de ellos es el método denominado SYN. Para utilizar el método SYN de Nmap, se pasa como parámetro la opción-sS. La ventaja radica en que no se llega a establecer una conexión TCP completa.

3. Detección de sistemas operativos: como se mencionó anteriormente, es muy útil identificar el sistema operativo del objetivo, mediante los puertos abiertos el analista puede sacar sus conclusiones. Por ejemplo, los puertos 135, 137, 139, o 445 a menudo indican que el objetivo tiene instalado un sistema operativo Windows. Sin embargo, si se desea obtener información más específica, se puede usar la opción-O de Nmap, que invoca al mecanismo de detección de sistemas operativos. Al momento de utilizar dicha opción, es necesario tomar las debidas precauciones dado que el mecanismo de detección utilizado por Nmap se basa en el envío de diferentes tipos de paquetes, algunos de ellos mal formados por lo que entonces la posibilidad de que algún sistema deje de responder ante la recepción de este tipo de paquetes.

4. Scripting engine (NSE): El motor de scripting de Nmap es una de sus funcionalidades más potentes y flexibles. Permite a los usuarios escribir (y compartir) scripts para automatizar una amplia variedad de tareas. Los analistas de seguridad pueden utilizar los scripts que se encuentran a disposición y que se distribuyen con Nmap, o escribir los suyos y de esta manera personalizar y automatizar su tarea. El NSE se activa con la opción-SC (o --script si desea especificar un conjunto personalizado de scripts), los resultados se integran con la salida normal de Nmap.

Zenmap: es la interfaz gráfica oficial de Nmap. Se trata de una aplicación multi-plataforma (Linux, Windows, Mac OS X) de libre distribución y de código abierto. El principal objetivo es facilitar el uso de Nmap para principiantes y proporciona características avanzadas para usuarios experimentados. Se pueden guardar perfiles con los análisis de uso frecuente, facilitando así la ejecución de tareas de uso frecuente.

AutoScan-Network: es un escáner de red, es útil tanto para la etapa de descubrimiento, como para la de identificación. No requiere configuración y el principal objetivo es obtener la lista de equipos conectados en una determinada red. Algunas de las características más importantes a destacar son: la detección automática de la red sin intervención humana no necesita privilegios de administrador, detección en tiempo real de equipos que se conectan a una red, detección de sistema operativo y de servicios, escáner SNMP y además cuenta con una interfaz gráfica amigable. Es útil cuando el analista de seguridad se encuentra posicionado dentro de la red y al no requerir de intervención humana, puede ser utilizada como una herramienta de primera línea y de esta manera generar una lista inicial de dispositivos activos. Luego se puede utilizar dicha lista para alimentar a herramientas más específicas, por ejemplo, Nmap con Script Engine.

5.4. La caracterización de vulnerabilidades

Esta etapa es efectuada posteriormente a la de reconocimiento y descubrimiento de objetivos. Una vez culminada dicha etapa el analista de seguridad tiene resultados que serán los insumos para armar un plan que conlleve a identificar, clasificar y verificar la existencia de vulnerabilidades. La precisión con la que se identifiquen los servicios y sistemas operativos juega un rol muy importante dado que cuanto más exacto sean los datos obtenidos, más eficacia en la verificación e identificación de vulnerabilidades tendrá el analista de seguridad.

Se debe entender por vulnerabilidad una característica o circunstancia de debilidad de un recurso informático la cual es susceptible de ser explotada por una amenaza (Zambrano, 2017). Por otro lado, el Instituto Nacional de Estándares y Tecnología de Estados Unidos indica que una vulnerabilidad es una falla o debilidad en los procedimientos de seguridad de un sistema, en el diseño, la implementación, o los controles internos que podrían ejercerse (accidentalmente disparado o explotado intencionalmente) y dar lugar a una brecha de seguridad o una violación de la política de seguridad del sistema (NIST, 2012).

El principal propósito de la etapa de caracterización de vulnerabilidades en esta guía es determinar las potenciales vías que tendría un agente malicioso para comprometer un objetivo, es decir para atacarlo. Posteriormente se clasifican las vulnerabilidades según el índice de compromiso al que conllevan las mismas. Dicho índice es determinado en cada caso, dependiendo de los activos involucrados y su relevancia. Es importante destacar que en esta etapa no es necesario constatar o manifestar el nivel de riesgos mediante pruebas empíricas, este paso queda para la etapa de explotación o ataque.

Como resultado de esta etapa se obtendrá una lista de las vulnerabilidades asociadas a los sistemas y procedimientos (fallas o debilidades), que potencialmente podrían ser explotada por fuentes de amenaza. Se recomienda crear una estructura tipo tabla que contenga al menos: la vulnerabilidad detectada, la fuente y el evento que activaría esa vulnerabilidad.

Es importante destacar que si es el caso de evaluar vulnerabilidades en los procedimientos se necesitan analistas de seguridad con una amplia experiencia y con una profunda comprensión de las tecnologías, procedimientos, legislación y las técnicas de ingeniería social utilizadas comúnmente por los agentes maliciosos y en el caso de evaluar las vulnerabilidades en los sistemas también se necesitan analistas competentes, entrenados y certificados, ya que, si bien existen herramientas automáticas, es necesario saber utilizarlas y además realizar un control cruzado en el análisis (Buendía, 2013).

La información obtenida en la etapa de reconocimiento y descubrimiento debe permitir que el analista de seguridad pueda afinar las herramientas a utilizar en esta etapa, con el fin de evitar contratiempos y centrarse en las cuestiones pertinentes a la etapa de identificación de vulnerabilidades. No es considerado una buena práctica utilizar las herramientas sin tener en cuenta la infraestructura a evaluar y la información recolectada anteriormente. El uso indebido o general de herramientas

aumenta considerablemente el número de falsos positivos y falsos negativos, y reduce la calidad de la evaluación, además de poder causar el mal funcionamiento de los servicios en cuestión.

5.4.1. Identificación de vulnerabilidades

El primer paso para realizar es la identificación de vulnerabilidades conocidas. En este paso se utiliza la información de puertos TCP/UDP abiertos, los banners asociados a los servicios, las firmas del sistema operativo y toda la información pertinente de las etapas anteriores. Se realiza el análisis de vulnerabilidad mediante el uso de herramientas automáticas a las cuáles se les suministra la información de encontrada en etapas previas, por ejemplo, la información de puertos TCP/UDP abiertos y así se evita que las herramientas realicen acciones innecesarias como las pruebas en puertos cerrados. También es importante tener en cuenta que las herramientas automáticas en general realizan pruebas de DoS (denegación de servicio) por lo que hay que tomar las medidas necesarias y todo debe haber quedado expresado y normado en la etapa de planificación. Como resultado tendremos una lista de vulnerabilidades que ya han sido descubiertas y divulgadas a través de sitios como el "Common Vulnerabilities and Exposures" y todas aquellas publicadas por las compañías oficiales propietarias de las aplicaciones y sistemas operativos (Franco, Perea, y Puello, 2012).

Es necesario señalar que los tipos de vulnerabilidades y la metodología necesaria para determinar la presencia de estas, en general varían dependiendo de la naturaleza del sistema y sus características. Si se están evaluando vulnerabilidades de sistemas operativos y aplicaciones ampliamente difundidas y utilizadas (servidores web, servidores SSH, bases de datos), posiblemente se puedan consultar fuentes que publiquen información referente a vulnerabilidades existentes. Si por el contrario se trata de una aplicación personalizada y que es utilizada por un único establecimiento es altamente probable que no existan fuentes de divulgación a los cuales acudir como referencia. Las auditorías sobre el código fuente y/o programas binarios pueden ayudar en la identificación de puntos vulnerables que no están disponibles en bases de datos de vulnerabilidad públicas. También hay que considerar los procesos manuales para la búsqueda de vulnerabilidades, en los cuales muchas veces es necesario confeccionar herramientas o instrumentos parad dichos fines.

Hay que tener en cuenta que se puede generar una vulnerabilidad cuando se configura de forma incorrecta un servicio y los procesos manuales pueden ayudar a detectar este tipo de problemáticas. Es importante confeccionar una lista de todas

las vulnerabilidades encontradas utilizando la información obtenida en los pasos anteriores, será una lista tentativa de vulnerabilidades.

El siguiente paso es realizar una depuración de la lista anterior para verificar la existencia de falsos negativos y positivos, en general esto se realiza mediante un proceso manual. Falsos positivos ocurren cuando, usando determinados criterios previamente definidos o estandarizados, se ha establecido la veracidad de una condición cuando la misma es falsa.

Por otro lado, el resultado de una prueba puede indicar que determinado servicio no es vulnerable, pero dependiendo de la realidad subyacente, el mismo puede presentar algún problema de seguridad. Un ejemplo puede ser el uso de protocolos sin criptografía, para determinados casos se considera correcto utilizar el protocolo HTTP sin cifrar, pero si se transmite información sensible, pasa a ser determinante el uso de HTTPS.

Por último, es recomendable hacer una lista final de vulnerabilidades con recomendaciones inmediatas donde se interpretan los resultados y se hace una lista final clasificada según la gravedad de las vulnerabilidades y la criticidad de los activos que afectan. Se Identifican las vulnerabilidades que requieren medidas de atención inmediatas y las contramedidas para su protección. Si existe un riesgo potencial alto se informa a las contrapartes inmediatamente.

5.4.2. Clasificación de vulnerabilidades

Las herramientas de escaneo de vulnerabilidades generalmente brindan algún tipo de salida clasificando las vulnerabilidades según un índice de riesgo. Sin embargo, para la organización destino un análisis basado en el impacto del negocio es más útil. Entrelazar las vulnerabilidades con el modelo de negocios dará un valor agregado al análisis, los resultados serán más comprensibles y facilitará el proceso de correcciones, así como también ayudará a justificar el presupuesto necesario para implementar las contramedidas (Solarte, 2015).

En otras palabras, no sólo se tienen que ejecutar las herramientas y entregar los informes generados. Es una mala práctica y les da poco valor a los resultados y al análisis en sí mismo. Consecuentemente, la organización evaluada se podría preguntar si no es más barato comprar/descargar y ejecutar las herramientas y obtener los mismos resultados.

Es importante preparar un resumen que contenga las vulnerabilidades clasificadas por dominios y/o componentes basados en un índice de riesgo, con base en proceso

de impacto en el negocio. Hay que tener en cuenta que esta clasificación puede diferir significativamente de una clasificación meramente técnica de los riesgos. Para poder clasificar desde el impacto en el negocio se requiere un conocimiento profundo de la organización de destino y sus procesos. Puede ser una buena técnica entregar un primer borrador que deba ser revisado por el personal de la organización evaluada para identificar correctamente el impacto en el negocio y los correspondientes ajustes que se deben hacer.

También es adecuado entregar un informe técnico que contenga los resultados reportados por las herramientas, pero con una explicación de estos y alguna medida del impacto técnico que potencialmente podría ocasionar a la organización. En pocas palabras, un informe especializado para la organización.

5.4.3. ¿Dónde consultar vulnerabilidades conocidas?

La información técnica y no técnica asociada a un determinado entorno se puede obtener a través de métodos de recopilación de información como los visto anteriormente. Una vez que se tiene la información suficiente, tales como los servicios y sus versiones, además de los sistemas operativos involucrados, se comienza a relacionar y analizar dicha información.

Para la identificación de vulnerabilidades en general es útil consultar fuentes de información, como, por ejemplo, páginas web de proveedores donde se publiquen errores y defectos de los sistemas o aplicaciones. Existen en Internet fuentes de información que divulgan vulnerabilidades sobre sistemas conocidos. Dichas fuentes deben ser tenidas en cuenta en un análisis de vulnerabilidades. Algunos referentes en esta área son:

- *National Vulnerability Database* (http://nvd.nist.gov/). Es un repositorio de datos del gobierno de los EE. UU. Basado en estándares de gestión de vulnerabilidades, representadas mediante el Security Content Automation Protocol (SCAP). Estos datos permiten la automatización de la gestión de vulnerabilidades.
- *Security-Database* (http://www.security-database.com). Proporciona una base de datos de vulnerabilidades, basada en estándares abiertos para la clasificación, calificación, enumeración y explotación. También proporciona un repositorio de herramientas de seguridad y auditoría.
- *Common Vulnerabilities and Exposures* (CVE) (http://cve.mitre.org/). Es una lista de vulnerabilidades de seguridad, que tiene como objetivo proporcionar

nombres comunes a problemas de conocimiento público. El objetivo de la CVE es facilitar el proceso de compartir datos de las vulnerabilidades entre herramientas, repositorios y servicios, con un sistema de "enumeración o identificación común."

- *SANS* (http://www.sans.org). Es una fuente de formación en seguridad, provee una base de datos de vulnerabilidades y también servicios de certificación en seguridad. Asimismo, desarrolla, mantiene y pone a disposición una colección de documentos de investigación sobre diversos aspectos de seguridad informática.

El proceso de búsqueda de vulnerabilidades en estas fuentes puede realizarse en forma manual o puede ser asistida por herramientas de identificación de vulnerabilidades. Muchas de estas herramientas alimentan sus motores de búsquedas utilizando información proveniente de fuentes públicas. Más adelante en esta sección se presentarán algunas de estas herramientas que evidentemente pueden apoyar este proceso.

5.4.4. Lista de requerimientos de seguridad

Dependiendo del tipo de análisis y de si el mismo incluye entrevistas de evaluación y levantamiento de datos, puede ser útil confeccionar cuestionarios y listas de chequeo específicas. Determinadas preguntas podrían ser efectivas para identificar vulnerabilidades que pueden ser aplicables a determinados sistemas y entornos, por ejemplo, una versión específica de un sistema operativo específico o si se transmite información sensible utilizando canales públicos.

En el mejor de los escenarios en las organizaciones existe personal encargado de la evaluación de riesgos o al menos debería ser el escenario deseable. Son los encargados de determinar y establece los requisitos de seguridad para los sistemas informáticos y los procedimientos. Asimismo, determinan los controles necesarios para evaluar el cumpliendo de dichos requisitos.

La información que pueda proveer la organización sobre sus activos y requisitos de seguridad es fundamental al momento de generar listas de chequeo para verificar el cumplimiento de requerimientos de seguridad. La realidad indica que muchas empresas no tienen personal dedicado exclusivamente a la seguridad informática y consecuentemente no tienen claramente identificados los activos críticos del negocio, ni los requisitos de seguridad. Es importante que el analista de seguridad tenga creadas listas de chequeo de requerimientos de seguridad generales, las que serán instanciadas apropiadamente en cada caso. Una lista de verificación de

requerimientos de seguridad contiene las normas que pueden utilizarse para evaluar e identificar de manera sistemática las vulnerabilidades sobre los activos (personal, hardware, software, información). Se recomienda clasificar en áreas de gestión o administración, de operación y técnicas.

5.4.5. Herramientas automáticas

Es importante utilizar herramientas y aplicaciones para el escaneo de vulnerabilidades que se encuentran muy maduras y que, además, muchas de ellas son open source o sofware libre permitiendo así tener más agilidad y eficiencia en la detección y clasificación.

- *Open Vulnerability Assesment System (OenVAS).* Es un framework compuesto por varios servicios y herramientas, entre ellas ofrece un escáner de vulnerabilidades orientado a redes e infraestructura. El escáner de vulnerabilidades es una aplicación cliente servidor, donde el cliente ofrece una interfaz gráfica para el usuario final. El servidor ofrece un conjunto de más de 19 mil pruebas que son utilizadas para detectar vulnerabilidades en sistemas y aplicaciones remotas. OpenVAS tiene licencia GPL y es un fork del escáner de vulnerabilidades Nessus, surge como alternativa cuando este último cambia la forma de licenciamiento. Luego que se ha obtenido una lista de hosts y servicios activos de la fase de identificación y descubrimiento, se puede pensar en ejecutar OpenVAS sobre los mismos (Drilling, 2012).
- *Nikto*. Es una herramienta de evaluación de servidores web. Está diseñada para buscar archivos y configuraciones por defecto que puedan comprometer a un servidor. Es una herramienta con licencia GPL, lleva a cabo pruebas exhaustivas sobre los servidores web, entre ellas se incluyen búsquedas de CGI vulnerables, controles de versiones no actualizadas y problemas conocidos sobre versiones específicas de servidores web. Es una herramienta que se debe utilizar con precaución, pues no está diseñada para ser cautelosa. Las evaluaciones sobre los servidores web se realizan en el menor tiempo posible. En general deja muchas entradas en los archivos de bitácoras y consecuentemente es fácilmente detectable. Además de detectar vulnerabilidades también identifica elementos que no necesariamente implican un problema de seguridad. Por ejemplo, información que la organización no sabe que se encuentra disponible en el sitio web (Mohammed, 2016).
- *W3af (Web Application Attack and Audit Framework)*. Es un proyecto de código abierto, que tiene como objetivo principal automatizar la detección y

explotación de las vulnerabilidades de aplicaciones web. Es una herramienta que puede ser extendida mediante el uso de plugins o complementos escritos en Python. El framework o marco de trabajo se divide en tres fases: descubrimiento, auditoría y ataque. Existen mecanismo de comunicación entre los complementos ya que la idea es que trabajen en forma colaborativa para lograr un objetivo. Brinda dos tipos de interfaz, una a modo consola y otra gráfica, también permite definir perfiles para cada tipo de evaluación que se quiera realizar (Qianqian y Xiangjun, 2014).

El principal propósito de esta etapa, como probablemente el lector pudo percibir, es determinar las potenciales vías que tendría un agente malicioso para comprometer un objetivo. Para ello se describió e ilustró un proceso que simplemente intenta mostrar una posible forma de abordar la tarea, cada analista de seguridad o equipo de evaluadores puede desarrollar su propio proceso.

También se enumeraron algunas metodologías y herramientas. Sin embargo, todo analista de seguridad que participe en una evaluación debe estar íntimamente familiarizado con todos los aspectos de la identificación y verificación de vulnerabilidades. Los analistas no pueden confiar únicamente en herramientas automáticas para identificar y explotar todas las vulnerabilidades de un objeto de evaluación. Las herramientas automáticas pueden ayudar a acelerar las tareas, pero los ingenieros deben entender las fortalezas y limitaciones de dichas herramientas.

Debido a la cantidad y variedad de tecnologías existentes los conocimientos necesarios para realizar una verificación de vulnerabilidades manual siguen en aumento, y es necesario ponerse al día constantemente. Es importante recordar que en las evaluaciones de seguridad inciden una gran cantidad de factores externos que afectan las herramientas utilizadas y, por lo tanto, en algún punto siempre es necesaria una intervención manual.

5.5. Explotación de vulnerabilidades

El principal objetivo que se persigue en esta fase es comprobar o refutar el impacto potencial de las vulnerabilidades detectadas en la fase anterior. De esta manera se busca obtener el control del sistema y lograr una prueba empírica o experimental de la problemática. Se utiliza toda la información que el analista tiene disponible en este momento y que proviene de las fases anteriores. En general, el éxito depende de la creatividad y la experiencia del analista, en como éste aplica la inventiva y muchas veces la imaginación, para relacionar y entrecruzar la información que tiene disponible.

Llevar a cabo esta fase es un proceso costoso en términos de recursos y tiempo, por ello muchas veces no se busca tomar control sobre el sistema y simplemente se detectan las vulnerabilidades y proponen soluciones para resolver los problemas.

5.5.1. Generalidades

En el mundo de la seguridad informática habitualmente se comenta que si se cuenta con el tiempo y los recursos suficientes cualquier sistema puede ser comprometido. En el contexto de una evaluación de seguridad, el tiempo es un bien preciado y en algunos casos simplemente puede ser demasiado costoso encontrar los métodos de explotación. Consecuentemente, es posible que un sistema no sea comprometido durante una evaluación de seguridad. Es tarea del director de un proyecto de evaluación de seguridad saber cuándo se cumplieron las metas y dar por concluido el servicio.

El propósito de esta parte del documento es conocer algunas técnicas y herramientas para la explotación de vulnerabilidades, pero en general no existen recetas. Dada una vulnerabilidad, elegir una prueba de concepto adecuada (PoC, por sus siglas en inglés) y seleccionar que herramienta aplicar no es siempre una tarea fácil. En general, este tipo de decisiones dependerá mucho de la experiencia del analista que lleve adelante la tarea y en algunas ocasiones será necesario desarrollar herramientas específicas.

Para entender este importante y crítico proceso para el éxito de una evaluación de seguridad, es importante familiarizarse con algunos conceptos:

Ataque: en este contexto se define ataque como el acto deliberado de tratar de eludir los controles de seguridad en un sistema para tomar el control, causar daño o acceder a información privilegiada (Vieites, 2011). Los ataques pueden ser activos o pasivos. Un ataque activo es un aquél en el que el atacante manipula el sistema y/o los datos. En un ataque pasivo el atacante sólo monitorea el sistema y/o registra datos.

Tipos de ataques: tratar de definir todos los tipos de ataques existentes no es una tarea razonable, ya que dependerá mucho del sistema objetivo. Lo que sí se puede hacer es definir los propósitos generales de los ataques.

La integridad: garantiza que la información no ha sido alterada de forma inesperada. La modificación o destrucción de la información, de forma maliciosa, puede producir pérdidas económicas en la organización.

La disponibilidad: significa que la información y los recursos están disponibles cuando se los necesite. A menudo, la disponibilidad es el elemento más importante para una organización, sobre todo si está orientada a servicios. La pérdida de disponibilidad se logra mediante ataques de denegación de servicios. Estos ataques tienen como objetivo desactivar el acceso temporalmente, y son usualmente motivados por razones económicas o políticas.

La confidencialidad: es la propiedad para prevenir la divulgación de información a personas o sistemas no autorizados. Por ejemplo, una transacción de tarjeta de crédito en Internet requiere que el número de tarjeta sea transmitido desde el comprador al comerciante. Si un atacante obtiene el número de la tarjeta se ha producido una violación de la confidencialidad.

Autenticación: es el proceso de identificar a alguien como un usuario legítimo de un sistema. Un atacante tiene como objetivo poner en peligro los mecanismos de autenticación y obtener acceso a un sistema como un usuario autorizado. Por ejemplo, el ataque podría llevarse a cabo mediante el descubrimiento de las credenciales de un usuario legítimo y después usarlas con intenciones maliciosas.

No repudio: es un concepto importante para cualquier transacción realizada con medios electrónicos. Con este término se refiere a que cada parte involucrada en una transacción no podrá negar su participación en la misma. En un intento de robar o causar daños, los atacantes tratan de hacerse pasar por usuarios legítimos y de esta manera engañar a la otra parte.

Con base en la información anterior, se pueden agrupar los ataques según sean dirigidos a la integridad, disponibilidad, confidencialidad, autenticación y no repudio, eso sí, con la salvedad de que un mismo ataque podría eventualmente afectar a más áreas. Un ataque de fuerza bruta sobre contraseñas de servidores o sistemas se puede clasificar como un ataque de autenticación, por ejemplo.

A continuación, algunos ataques comúnmente conocidos:

Man in the middle attack (MITM), es un ataque mediante el cual el atacante se posiciona entre el emisor y receptor de una comunicación. Este ataque podría comprometer la autenticación, la integridad, confidencialidad y el no repudio.

Ataques de inyección, es un ataque basado en el procesamiento invalido de datos. Ejemplos son SQL Injection y Shell Injection. Con este ataque, por ejemplo, se podría comprometer la integridad y la autenticación.

Ingeniería social, es un ataque destinado a obtener información confidencial a través de la manipulación de usuarios legítimos. Aquí se estaría comprometiendo, por ejemplo, la confidencialidad y la autenticación.

Escalar privilegios, en un esquema con múltiples roles, esto es realizar acciones, con un usuario de un determinado rol, con el fin de aumentar los privilegios de dicho usuario, o apoderarse de otro que se encuentre en un rol con mayor nivel de acceso en el sistema. Acá se pueden clasificar en privilegios horizontales y verticales, así es pues escalar de un usuario con limitados privilegios a un usuario con más privilegios, sería una escalada vertical.

En este punto es importante resaltar también el tipo de atacante que podría ejecutar acciones como las anteriormente mencionadas, en general, hay dos tipos de intrusos que representan una amenaza a la seguridad, atacantes externos e internos a la organización. Si bien siempre se tiende a pensar en los atacantes siempre son agentes externos, estudios de diversas empresas dedicadas a la Seguridad Informática indican que del 70 al 80 por ciento de los ataques son originados dentro de la organización atacada. En este contexto, cada empleado es una amenaza potencial para la organización. En general, un usuario interno puede atacar por múltiples razones, incluyendo el robo de datos para venderlos a la competencia o el sabotaje.

5.5.2. Ejecución

En la fase de explotación el analista o evaluador de seguridad, al igual que un atacante, eludiendo las medidas de seguridad tratará de obtener algún tipo de acceso no autorizado. Si lo logra, y como segunda medida, realizando una escalada de privilegios tratará de obtener un mayor nivel de privilegios. Para tal efecto, se recomiendan los siguientes pasos:

- *Comprobar o refutar la existencia de vulnerabilidades*: una vez que se tiene la lista de posibles vulnerabilidades, proveniente de fases anteriores, se utilizan herramientas para intentar obtener la mayor cantidad de puntos de accesos no autorizados.
- *Desarrollar herramientas y scripts:* para determinadas vulnerabilidades muchas veces se pueden encontrar en fuentes públicas herramientas que faciliten el ataque, por ejemplo, scripts o binarios desarrollados por terceros. En otras ocasiones no se encuentran herramientas y es por lo tanto necesario desarrollarlas, tal y como se ha mencionado anteriormente en esta guía.

- *Probar las herramientas en un entorno aislado*: cualquiera que sea la situación, es necesario probar a fondo la herramienta a utilizar en un entorno aislado y luego en la infraestructura del cliente. Si la herramienta es desarrollada por terceros hay que asegurarse de que se cuente con una versión actualizada de la misma.
- *Encontrar una prueba de concepto (PoC):* para que la organización que solicita el servicio pueda comprender el nivel de impacto que tiene determinada vulnerabilidad es necesario elegir una buena prueba de concepto. Para ello, el analista necesita conocer el modelo de negocios de la organización. Dependiendo del tipo de evaluación, esta información se la puede proporcionar el auditor al ingeniero de seguridad. En otras ocasiones, en base a la información de reconocimiento, el ingeniero de seguridad tendrá que decidir qué prueba elegir.
- *Documentar los hallazgos:* por último, es necesario documentar los hallazgos y los momentos (día y hora) en que fue realizada cada intrusión. Esto permitirá, en caso de que sea pertinente, evaluar los sistemas de control de la organización (alarmas, sistema de bitácoras, entre otros).
- *Intento de escalada de privilegios*: si se logró algún tipo de acceso y si el alcance del servicio así lo indica, una táctica para elevar privilegios implica buscar vulnerabilidades adicionales en el sistema, pero ahora desde una perspectiva interna. Si se obtiene un acceso a un sistema, incluso si el acceso es limitado, se pueden explotar las vulnerabilidades que son accesibles sólo como un usuario registrado. Hay que tener en cuenta que las defensas externas son a menudo más fuertes que los controles internos. Este es un ciclo continuo, en el cual se puede volver a una fase anterior, como la de análisis de vulnerabilidades. A menudo el enfoque del servicio de análisis es de caja gris y los analistas de seguridad parten de un usuario con mínimos privilegios. Otra técnica para intentar elevar los privilegios es husmear (sniffing) en la red en busca de nombres de usuario y contraseñas. También se podría aplicar ingeniería social, pero esto sólo si es explícitamente solicitado por la organización.

Para la explotación existen diversas herramientas que han sido desarrolladas por la comunidad de desarrolladores de software libre mundial que tienen excelentes funcionalidades y son utilizadas muy frecuentemente en evaluaciones de seguridad. Algunas referencias son las siguientes:

- *Metasploit Framework (MSF).* Es un entorno completo para escribir, probar y usar el código orientado a la explotación de vulnerabilidades. Proporciona

una plataforma sólida para pruebas de penetración, para el desarrollo de shell code y para la investigación de vulnerabilidades. Las principales características que le dan una ventaja a MSF frente a otras opciones son: soporte para extender herramientas, bibliotecas, debugger, encoding y, además, provee una API modular y extensible a los desarrolladores, es mutiplataforma y tiene soporte para diversos protocolos de red incluyendo una variedad de "exploits" para vulnerabilidades conocidas (Holik, 2014).

- *Hydra.* Es una herramienta que permite implementar ataques de fuerza bruta sobre la contraseña y usuario de inicio de sesión de múltiples servicios (Ghanem, 2015). Entre los servicios a los cuales se brinda soporte se encuentran: TELNET, FTP, HTTP, HTTPS, HTTP Proxy, SMB, SMBNT, MS SQL, MySQL, rexec, rsh, rlogin, CVS, SNMP, SMTP-AUTH, SOCKS5, VNC, POP3, IMAP, NNTP, PCNFS, ICQ, SAP R / 3, LDAP2, LDAP3, Postgres, entre otros (Najera-Gutierrez y Ansari, 2018).

Al término de esta fase lo más probable es que el evaluador de seguridad haya adquirido un claro entendimiento de las fortalezas y debilidades de seguridad del sistema analizado. La parte práctica de la evaluación se encuentra en su etapa final, posiblemente los ingenieros se unirán al conjunto de documentadores para comenzar a trabajar en el informe final. Es importante recordar que el objetivo general en una evaluación no es poner en peligro al sistema o red, es informar a los clientes en cuanto a las vulnerabilidades existentes en su sistema.

Si el alcance así lo indica, una vez que tenemos un compromiso inicial sobre un sistema se deben buscar maneras de aumentar los privilegios de acceso. A modo de ejemplo, si se logra acceso a la red local, se debe deben buscar maneras de convertirse en un administrador. También hay que analizar el tráfico en la red buscando toda la información sensible que se pueda obtener.

Debido a que el compromiso total de un sistema tiene un gran atractivo dentro de las evaluaciones de seguridad, los ingenieros tienden a solicitar tiempo adicional para llevar adelante nuevos ataques. Aquí es donde el director del equipo tiene que intervenir y evaluar si se cumplieron los objetivos que se plantearon en la propuesta, o es necesario seguir realizando tareas adicionales. Si la nueva vulnerabilidad promete aumentar el acceso al sistema, el director aplicará técnicas de gestión de proyectos que permitirán lograr acuerdo sobre el uso de tiempo adicional para dicha actividad.

5.6. Informe de la evaluación de seguridad

Es aquí donde se consolida la un proceso sistemático, planificado y técnicamente bien ejecutado y profesionalmente coordinador, ya que la documentación constituye la principal relación entre los resultados de las fases de revisión y ejecución, el analista y el objeto de evaluación. Aunque desde el punto de vista técnico el trabajo a desarrollar en esta fase pueda ser poco atractiva, un analista de seguridad debe tener bien claro el alto nivel de importancia y sensibilidad inherentes a los datos que deben ser documentados. Los documentos generados en esta fase no se limitan a exponer potenciales vulnerabilidades de un objeto de evaluación, los mismos pueden inclusive ser considerados como, al menos parte de, evidencia de que la organización satisface (o no) determinadas políticas de seguridad ya sean propias de la organización o derivadas de marcos normativos o estándares de seguridad (Fernández y Casas, 2017).

Es importante remarcar que una gran medida del éxito de esta fase depende de la precisión y detalle con el que el analista ha anotado, paso por paso, los procedimientos aplicados y los correspondientes resultados. El principal valor agregado de lo que se documenta es permitir a aquellos que, son los encargados de asegurar el buen funcionamiento de los sistemas, aplicar los patrones de ataque y poder verificar/validar los resultados obtenidos durante el análisis desarrollado. Es esencial que la organización esté consciente de: la forma de operación de un atacante o algún tipo de atacante, las técnicas y herramientas utilizadas por el atacante, cómo pueden ser explotadas las vulnerabilidades identificadas y además ser conscientes de cualquier exposición innecesaria de datos que pueda estar presentando la organización.

Es altamente probable que el personal de la organización analizada no implemente ataques simulados basándose en los descubrimientos documentados, y que sólo se limite a reproducir algún comportamiento simple y se concentre en remediar los problemas detectados. También es probable que el analista no necesite describir en detalle cómo llegó a los descubrimientos sino proveer el detalle de estos.

Asumiendo que el analista ha hecho un buen trabajo en descubrir y explotar vulnerabilidades identificadas en el objetivo de evaluación, y de que ha tomado nota de los procesos efectuados, un punto esencial es poder presentar en forma convincente la interrelación y consistencia de estos. Ninguna herramienta es 100% exacta, por lo tanto, la verificación de lo que es presentado como resultado de la evaluación es un punto crítico. Es esta precisión lo que va a generarle confianza a la organización con relación a la actuación del analista de seguridad. La integridad

de los datos que se le presenta a la organización es fundamental, no hay lugar a inexactitudes o falsos positivos.

Una vez efectuadas las pruebas de seguridad, el analista usualmente cuenta con una gran cantidad de datos, desde tomas de pantalla (screenshots) y observaciones manuales que han sido documentadas hasta reportes detallados generados por las diversas herramientas utilizadas para desarrollar las pruebas, por lo tanto ¿qué se debe hacer con todos estos datos?

Un primer paso es naturalmente revisar cuidadosamente los datos obtenidos tratando de identificar y remarcar el alcance e impacto de estos. Este proceso puede estar guiado por los siguientes criterios: rankings de vulnerabilidades provistos por las herramientas de evaluación, los conocimientos profesionales del analista de seguridad (juicio de experto y criterios de no conformidad) y el contexto de la vulnerabilidad detectada (Ruiz Gómez, 2018).

Una vez que hayan sido validados los resultados y generadas las evidencias correspondientes es necesario generar la documentación final con el objetivo de presentar el resultado del análisis de seguridad a la organización. Naturalmente, existen varias formas posibles de documentar y presentar la información resultante del análisis, pero las secciones siguientes se consideran imprescindibles en un documento de este tipo.

5.6.1. Resumen ejecutivo y análisis general

Es típicamente la primera sección del informe y consiste en un resumen de alto nivel que está dirigido principalmente a la Junta Directiva de la organización, el director ejecutivo, director de operaciones o al director de tecnologías de información. Estos actores aun cuando estén sumamente interesados por los resultados del análisis, no desean, en general, entender en detalle cómo el analista logró vulnerar una aplicación crítica usando un ataque de Cross Site Scripting (XSS), por ejemplo. Por lo tanto, el resumen ejecutivo debería incluir estadísticas y un diagnóstico preciso del estado de la seguridad del objetivo de la evaluación.

En el resumen ejecutivo también una presentación bien estructurada de estadísticas de los resultados es sumamente útil, en particular cuando el reporte incluye el análisis de diferentes objetivos de evaluación. Si hay solamente un objetivo de evaluación, entonces es particularmente relevante proveer una representación de las estadísticas globales usando, por ejemplo, tablas que incluyan al menos el nivel de severidad (bajo, medio, alto, crítico), la cantidad de vulnerabilidades descubiertas por cada

nivel de severidad y la cantidad recursos que son afectados por esas debilidades, por ejemplo, una vulnerabilidad Cross Site Scripting (XSS) podría ser una vulnerabilidad que afecte a múltiples sitios web de la organización. Así pues, también es importante hablar en términos porcentuales de los niveles de severidad. Los datos estadísticos permiten establecer una medida general del estado de la situación a los cuadros directivos de la organización.

En la sección de Análisis el objetivo es respaldar esos números con datos relevantes. Por ejemplo, si el objeto de evaluación tiene la mayoría de las instancias en el nivel de severidad "Bajo" entonces se debería remarcar el hecho de que el objeto está operando sin riesgos sustanciales para la entidad propietaria del mismo. Es muy importante resumir los resultados de forma simple y lo más directa posible.

Es en esta sección donde también se presenta la oportunidad de educar a los receptores del informe, por ejemplo, con relación a las mejores prácticas de la industria vendría bien. Sin embargo, esta sección debe ser usada con ese objetivo solamente si los datos con los que se cuenta son relevantes. Esto significa que si no hay susceptibilidad particular con relación a alguna mejor práctica entonces es preferible no mencionar el tema. Es importante asegurarse que todo tema que sea planteado revista un impacto sustancial y que efectivamente pueda afectar el objetivo analizado.

5.6.2. Riesgos detectados y clasificados

El mapeo de los riesgos es el componente más importante del informe. Es aquí donde los descubrimientos que han sido verificados son reportados utilizando una matriz de riesgos que cuantifique todos los descubrimientos y las vulnerabilidades verificadas, que categorice los problemas identificados e identifica los recursos potencialmente afectados. Por otro lado, es importante presentar todos los detalles relevantes de los resultados de las evaluaciones, proveer referencias, sugerencias y recomendaciones relevantes.

Los datos pueden ser presentados en el formato que se considere más adecuado o incluso si la organización lo solicitó con algún formato en específico en la fase de planificación, pero es una buena práctica que los mismos sean presentados en un formato tabular simple y fácil de entender, si es posible con impacto gráfico. A continuación, se describen las secciones que en su conjunto van a permitir estructurar la comunicación de los descubrimientos a la organización receptora del informe.

¿Qué son los niveles de severidad? Son usados para categorizar los descubrimientos son: Crítico, Alto, Medio, Bajo e Informativo. Es claro que la categorización de severidad otorgada a un hallazgo de la evaluación de seguridad es un hecho completamente subjetivo y fuertemente ligado a la experiencia del analista (juicio de experto) y al propio objeto de evaluación (Polanía, 2016).

El Nivel Crítico puede ser utilizado para las vulnerabilidades o riesgos:

- Cuyo objetivo de evaluación sea expuesto a ataques de denegación de servicios (DoS, por si siglas en inglés) o ejecución de comandos maliciosos.
- Que la vulnerabilidad pueda ser revelar información privada o sensible.
- Que los riesgos puedan ser explotados con muy poco conocimiento y esfuerzo por parte de un atacante.

El Nivel Alto puede ser utilizado para las vulnerabilidades o riesgos:

- Que revelen código fuente de aplicaciones que se ejecutan en los servidores de la organización.
- Donde se exponga, en forma innecesaria y por una inadecuada gestión de errores, información que pueda facilitar ataques de nivel crítico.
- De que un atacante pueda fácilmente apropiarse de forma ilegítima de recursos de la infraestructura web.
- Estos riesgos puedan ser explotados con algo de conocimiento y esfuerzo por parte de un atacante.

El Nivel Medio puede ser utilizado para las vulnerabilidades o riesgos:

- Que exponen en forma innecesaria datos no críticos del sistema evaluado.
- Que revelen datos protegidos que no han sido categorizados como privados o sensibles.
- Que requieren un esfuerzo y conocimiento sustancial por parte del atacante.

El Nivel Bajo puede ser utilizado para las vulnerabilidades o riesgos:

- Que pueden ser usadas para construir ataques de mayor nivel de severidad, pero no en forma directa.
- Que revelan información, pero requieren un conocimiento interno y muy cercano del objeto de evaluación.

- Que pueden ser usadas para construir ataques de mayor nivel de severidad, pero solamente si el atacante posee un conocimiento extremadamente sofisticado.

El Nivel Informativo puede ser utilizado para las vulnerabilidades o riesgos:

- Información expuesta que directamente no representa, ni permite explotar, una vulnerabilidad.
- Información expuesta que no es de naturaleza técnica y que se considera pertinente reportar a la organización

5.6.3. Indicación de los elementos afectados y recomendaciones

En esta sección del informe se listan todos los recursos dentro del alcance del objetivo de evaluación afectados. Desde un punto de vista organizacional deben ser listados por tipo de problema y deber ser resumidos todos los problemas identificados usando toda la información que se considere necesaria para el entendimiento de estos.

Se debe explicar al receptor del informe todas las consecuencias que puede implicar una vulnerabilidad detectada y documentada de todos los elementos afectados. A menudo individuos pertenecientes a la organización poseen cierto conocimiento de la existencia de problemas, pero pueden no tener una idea clara de las consecuencias que podría tener que determinada vulnerabilidad sea explotada.

Es importante proveer referencias por cada elemento afectado que permitan respaldar los descubrimientos y que le provean, por ejemplo, a un equipo de técnicos que sea el encargado de resolver los problemas información adicional acerca del problema en cuestión. En esta parte del informe puede incluir también referencias a pautas de requerimientos de conformidad del objetivo de evaluación (por ejemplo, controles COBIT/ISO27002).

Acá se puede crear una tabla que incluya secciones como la problemática encontrada y una descripción de la vulnerabilidad bien detallada, las referencias que fundamenten el hallazgo y por supuesto, la evidencia. También es importante indicar recomendaciones profesionales cuya implementación permita solucionar problemas identificados de la mejor manera.

Dentro de esta sección caerán bien una serie de recomendaciones de mejores prácticas para proveer un gran valor agregado a la evaluación de seguridad realizada. Es importante tener en cuenta que aún desarrolladores o administradores

de infraestructura expertos pueden sentirse desconcertados por algunos de los descubrimientos reportados.

Ejemplos:

- Proveer a los técnicos algún tipo de conocimiento básico que les permita comenzar a entender cómo resolver el problema.
- Ejemplo de codificación, donde se presentan buenos y malos códigos, son generalmente un buen punto de comienzo para el caso de vulnerabilidades en aplicaciones.
- Manejo elegante de errores, donde no se expone ningún dato clave, es también esencial, ya que es una fuente usual de revelamiento de información, por ejemplo, cuando se envía información no sanitizada de error a través de un navegador de Internet u otro cliente HTTP (Cuevas *et al*., 2018).

Obviamente que es responsabilidad y decisión del equipo de remediación aplicar estas recomendaciones y el uso de estas es completamente relativo al objetivo de evaluación.

5.6.4. Evidencias y documentos generados

Este tipo de entregables resultandos durante el desarrollo del análisis deben ser asegurados con máxima diligencia. En esencia, los resultados obtenidos por el analista podrían ser de suma utilidad para un posible atacante. La información recopilada representa un riesgo desde el punto de vista de la susceptibilidad a ataques maliciosos de la organización. Estos documentos deben ser protegidos. Si se decide hacerlos disponibles en forma remota es fundamental tomar los recaudos de que el mecanismo de publicación no sea susceptible a todas las fuentes de ataques que se han visto en este capítulo. Los mecanismos de control de acceso y de encriptación utilizados deben ser de excelente calidad.

Debe ser considerado seriamente el utilizar cifrado fuerte sobre el conjunto total de los entregables. No se debería entregar ningún documento o evidencia que no haya sido se haya cifrado. Para eso, es importante además haber sincronizado con el personal de la organización el método y herramienta utilizada para implementar el aseguramiento de la información. Si es necesario intercambiar claves, el proceso debería ser realizado en forma off-line.

5.6.5. ¿Cómo presentar el informe?

La presentación de los hallazgos realizados durante la evaluación de seguridad debe ser guiada por un simple objetivo: tener un claro y preciso entendimiento por parte de la audiencia. Para esto hay que enfocarse en:

- Las capacidades y el conocimiento técnico de la audiencia.
- Los objetivos de la organización.

Naturalmente, un analista de seguridad reportando el resultado de su trabajo va a enfrentarse a audiencias con capacidades técnicas diferentes. Si no se es capaz de adaptar el material que conforma la presentación de resultados a la audiencia que los recibe, el éxito de la tarea se puede ver amenazado. La gente, usualmente, reacciona en forma muy diferente ante un mismo segmento de información. Una clave importante del trabajo del analista es lograr que la audiencia logre contextualizar los riesgos identificados en relación con su rol e intereses. Por ejemplo, los cuadros directivos no técnicos de la organización no necesariamente tendrán interés en comprender cómo efectivamente funciona un vector de ataque explotando un XSS contra las aplicaciones web de la organización, que haya sido construido por el analista. Sin embargo, es fundamental poder transmitirle a ese perfil de audiencia los riesgos a los que se ve expuesta la organización y cuál es el esfuerzo/costo requerido para poder remediar la vulnerabilidad identificada. Asimismo, posiblemente ellos sean conscientes de las implicaciones legales de no tomar acciones correctivas a la luz de los resultados del trabajo desarrollado por los analistas de seguridad.

Una presentación basada en diapositivas y con estadísticas del resumen ejecutivo del documento que reporta el resultado del análisis es generalmente muy bien recibido por aquellos que son los responsables de haber contratado el servicio.

Por otro lado, aun cuando este no sea el caso general, es muy posible que el analista también tenga que presentar sus resultados a un equipo de técnicos, posiblemente miembros del equipo de remediación, de la organización. En este caso, una presentación orientada a reproducir o simular, paso a paso, algunos de los ataques que el analista haya sido capaz de montar en vivo suele tener un factor de eficacia muy alto. Este tipo de presentación, sin embargo, debe ser realizada con mucho tacto y en forma precisa. Es muy importante entender el nivel de habilidades técnicas, así como poder captar y gestionar el potencial nivel de resentimiento que estos técnicos puedan tener hacia un analista y las funciones que cumple desde ese rol. Algunos desarrolladores de software pueden visualizar a un analista de seguridad como aquel cuyo objetivo principal es descubrir y exponer las deficiencias en su trabajo.

Este sentimiento es altamente entendible y el analista debe tener la capacidad de posicionar ante el mismo y convencer a su audiencia que en realidad su trabajo es una contribución al de ellos y que incluso su actividad debería ser considerada como una extensión de la del equipo. Otros desarrolladores, verán al rol del analista como muy importante y crítico, ya que ellos no tienen el tiempo para realizar las tareas que exige ese rol.

De todas formas, lo esencial es que el analista al presentar el resultado de su trabajo adopte una postura totalmente profesional y exenta de emociones o subjetividad, remitiéndose a trabajar sobre los problemas identificados, probándolos y tratando de trabajar con la gente relevante para tratar de remediar los mismos.

CAPÍTULO VI: CONCLUSIONES

Solera *et al*. (2015) afirman que "(…) las pruebas con software y el monitoreo de los sistemas de información permiten establecer el estado actual de la organización, identificar las causas de vulnerabilidades y proponer soluciones de control que permitan su mitigación" (p. 493).

No importa qué tipo de sistema se esté evaluando, es recomendable realizar siempre la etapa de identificación y descubrimiento antes de llevar adelante otra actividad o profundizar en la evaluación.

Durante la fase de descubrimiento e identificación se comienza a recopilar información específica de los objetivos de análisis, se obtienen datos de puertos abiertos y posiblemente los servicios que ofrecen. La información obtenida durante esa fase también se utiliza tradicionalmente para determinar el sistema operativo (o la versión de firmware) de los dispositivos evaluados.

El principal objetivo de esta fase es generar una lista de objetivos activos y de servicios que se ofrecen y son alcanzables desde la posición del evaluador. Dicha lista será utilizada en las siguientes fases para la identificación de vulnerabilidades, cuanto más exacta sea la identificación de dichos objetivos mejores resultados se obtendrán.

Se expusieron los argumentos que permiten determinar la extremada importancia que tiene el verificar los resultados que se han recolectado.

El analista de seguridad no puede, a priori confiar en nadie, por lo tanto, es esencial que él mismo use todas las técnicas que se han expuesto con el objetivo de desarrollar un proceso de validación y verificación total de los descubrimientos.

Una vez que los resultados han sido verificados los mismos deben ser cuidadosamente documentados, y estos documentos deben ser protegidos de sobremanera. El documento de reporte de resultados, como se ha visto, está estructurado a partir de diferentes secciones, las que generalmente están dedicadas a diferentes audiencias dentro de la organización objetivo.

El resumen ejecutivo contiene ejemplos numéricos y estadísticas. Se presentó cuál es el tipo de datos que es beneficioso presentar a las contrapartes técnicas de la organización objetivo. En definitiva, la matriz-tabla debe ser de utilidad para las personas que estarán a cargo de desarrollar las acciones correctivas que permitan remediar los problemas detectados.

Una vez que todo lo anterior haya sido completado, la presentación en forma presencial de los mismos constituye una fase muy importante, donde el analista puede contestar preguntas de la audiencia y posiblemente presentar evidencia formal sobre cómo se llegó a los descubrimientos reportados. Nuevamente, la presentación de los datos debe ser adaptada al tipo de audiencia, para lo que se dieron algunas guías elementales para este proceso.

La ejecución de evaluaciones de seguridad requiere de expertos con un amplio conocimiento y profunda experiencia en las últimas amenazas o vulnerabilidades descubiertas y que además conozcan las medidas de seguridad para combatirlas; de ahí la importancia de contar con un equipo preparado, capacitado, certificado y con claridad del alcance a realizar.

REFERENCIAS BIBLIOGRÁFICAS

Baloch, R. (2017). *Ethical hacking and penetration testing guide.* Auerbach Publications.

Benchimol, D. (2011). *Hacking desde cero*. Fox Andina en coedición con Gradi S.A. 14-30. http://www.tugurium.com/docs/HakingCero.pdf

Bracho-Ortega, C., Cuzme-Rodríguez, F., Pupiales-Yépez, C., Suárez-Zambrano, L., Peluffo-Ordóñez, D., y Moreira-Zambrano, C. (2017). Auditoría de seguridad informática siguiendo la metodología OSSTMMv3: caso de estudio. *Maskana, 8,* 307-319. https://publicaciones.ucuenca.edu.ec/ojs/index.php/maskana/article/view/1471

Buendía, J. F. R. (2013). *Seguridad informática.* McGraw-Hill.

Cano, J. J. (s.f.). *Auditoría de Seguridad, Evaluación de Seguridad y Pruebas de Penetración: Tres Paradigmas en la Seguridad Informática*. Helguero Asociados. https://www.helasconsultores.com/data/documentos/Microsoft%20Word%20-%2058_auditoria_seguridad.pdf

Cuevas, J. C., Muñoz, R. M., Di Gionantonio, M. A., Gastañaga, I., Gibellini, F., Parisi, G., Barrionuevo, D., y Cárdenas, M. Z. (2018). Análisis de Vulnerabilidades de Sistemas Web en desarrollo y en producción. In *XX Workshop de Investigadores en Ciencias de la Computación (WICC 2018, Universidad Nacional del Nordeste)*. http://sedici.unlp.edu.ar/handle/10915/68347

Drilling, T. (2012). Seguridad en la Red: escáner de vulnerabilidades OpenVAS. *Linux magazine,* (88), 28-33. https://dialnet.unirioja.es/servlet/articulo?codigo=4083570

Estupiñan, A. D. C. A., Pulido, J. A., y Jaime, J. A. B. (2013). Análisis de Riesgos en Seguridad de la Información. *Ciencia, innovación y tecnología, 1,* 40-53.

Fernández, D. A. A., y Casas, X. C. (2017). Auditoría informática: un enfoque efectivo. *Dominio de las Ciencias, 3*(3), 157-173. https://dialnet.unirioja.es/servlet/articulo?codigo=6102836

Franco, D. A., Perea, J. L., y Puello, P. (2012). Metodología para la Detección de Vulnerabilidades en Redes de Datos. *Información tecnológica, 23*(3), 113-120. http://dx.doi.org/10.4067/S0718-07642012000300014

Franco, D. C., y Guerrero, C. D. (2013). Sistema de Administración de Controles de Seguridad Informática basado en ISO/IEC 27002. In *11th Latin American and Caribbean Conference for Engineering and Technology (pp. 1-10).* http://www.laccei.org/LACCEI2013-Cancun/RefereedPapers/RP239.pdf

Ghanem, M. A. (2015). BackTrack System: Security against Hacking. *International Journal of Scientific and Research Publications, 5*(2), 1-4. http://www.ijsrp.org/research-paper-0215/ijsrp-p3882.pdf

Hallberg, J., Hunstad, A., y Peterson, M. (2005). A framework for system security assessment. In *Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop, West Point, NY, USA, (pp. 224-231)*. https://doi.org/10.1109/IAW.2005.1495956

Hernández, G. H. (2014). Protocolo de Control de Transferencia (TCP). *Ciencia Huasteca Boletín Científico de la Escuela Superior de Huejutla, 2*(3). https://www.uaeh.edu.mx/scige/boletin/huejutla/n3/r1.html

Herzog, P. (2003). *Open-source security testing methodology manual.* Institute for Security and Open Methodologies (ISECOM).

Holik, F., Horalek, J., Marik, O., Neradova, S., y Zitta, S. (2014). Effective penetration testing with Metasploit framework and methodologies. In *2014 IEEE 15th International Symposium on Computational Intelligence and Informatics (CINTI), Budapest, Hungary, (pp. 237-242).* https://doi.org/10.1109/CINTI.2014.7028682

Jagatic, T. N., Johnson, N. A., Jakobsson, M., y Menczer, F. (2007). Social phishing. *Communications of the ACM, 50*(10), 94-100.

López, P. A. (2010). *Seguridad informática.* Editex.

Mohammed, R. (2016). Assessment of web scanner tools. *International Journal of Computer Applications, 133*(5), 1-4. https://pdfs.semanticscholar.org/cd74/8e04a04219849f31b70d8fb9236da6520af8.pdf

Najera-Gutierrez, G., y Ansari, J. A. (2018). *Web Penetration Testing with Kali Linux: Explore the methods and tools of ethical hacking with Kali Linux.* Packt Publishing Ltd.

National Institute of Standards and Technology. (2012). *Risk Management Guide for Information Technology Systems,* Special Publication 800-30. CSD. National Institute of Standards and Technology.

Patiño, S., Mosquera, C., Suárez, F., y Nevarez, R. (2017). Evaluación de seguridad informática basada en ICREA e ISO27001. *Universidad Ciencia y Tecnología, 21*(85). https://www.researchgate.net/publication/325191433_EVALUACION_DE_SEGURIDAD_INFORMATICA_BASADA_EN_ICREA_E_ISO27001

Pinzón, L., Talero, M., y Bohada Jaime, J. (2013). Pruebas de intrusión y metodologías abiertas. *Ciencia, Innovación Y Tecnología, 1,* 25-38. https://www.jdc.edu.co/revistas/index.php/rciyt/article/view/120

Polanía, G. A. S. (2016). Metodología para el análisis de vulnerabilidades. *TIA Tecnología, investigación y academia, 4*(2), 20-28.

Qianqian, W., y Xiangjun, L. (2014). Research and design on Web application vulnerability scanning service. In *2014 IEEE 5th International Conference on Software Engineering and Service Science, Beijing, China, (pp. 671-674).* https://doi.org/10.1109/ICSESS.2014.6933657

Ramos, M. D. P. A., y Hurtado, A. G. C. (2011). *Seguridad informática* (11ª ed.). Editorial Paraninfo.

Ruiz Gómez, J. C. (2018). *Formación de auditores internos ISO27001 y técnicas de Hacking ético*. http://repository.unipiloto.edu.co/handle/20.500.12277/4648

Solarte, F. N. S., Rosero, E. R. E., y del Carmen Benavides, M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica-ESPOL, 28*(5). http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456

Stoneburner, G., Goguen, A., y Feringa, A. (2002). *Risk management guide for information technology systems. Recommendations of the National Institute of Standards and Technology.* Special Publication, 800-30. National Institute of Standards and Technology. https://www.archives.gov/files/era/recompete/sp800-30.pdf

Tejada, E. C. (2015). *Auditoría de seguridad informática. IFCT0109.* IC Editorial.

Tejada, E. C. (2015). *Gestión de incidentes de seguridad informática. IFCT0109.* IC Editorial.

Urbina, G. B. (2016). *Introducción a la seguridad informática*. Grupo editorial PATRIA.

Vieites, Á. G. (2011). *Enciclopedia de la seguridad informática* (Vol. 6). Grupo Editorial RA-MA.

Walker, M. (2011). *CEH Certified ethical hacker all-in-one exam guide.* McGraw-Hill Osborne Media.

Zambrano, S. M. Q., y Valencia, D. G. M. (2017). Seguridad en informática: consideraciones. *Dominio de las Ciencias, 3*(3), 676-688. https://dialnet.unirioja.es/servlet/articulo?codigo=6137824

TIC's

3ciencias