UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Implementación de metodología PTES en auditorías de seguridad informática

INFORME DE ACTIVIDADES PROFESIONALES

Que para obtener el título de

Ingeniero en Computación

P R E S E N T A

Luis Miguel Torres Ortiz

ASESOR DE INFORME

Ing. Alberto Templos Carbajal

Ciudad Universitaria, Cd. Mx., 2019

AGRADECIMIENTOS

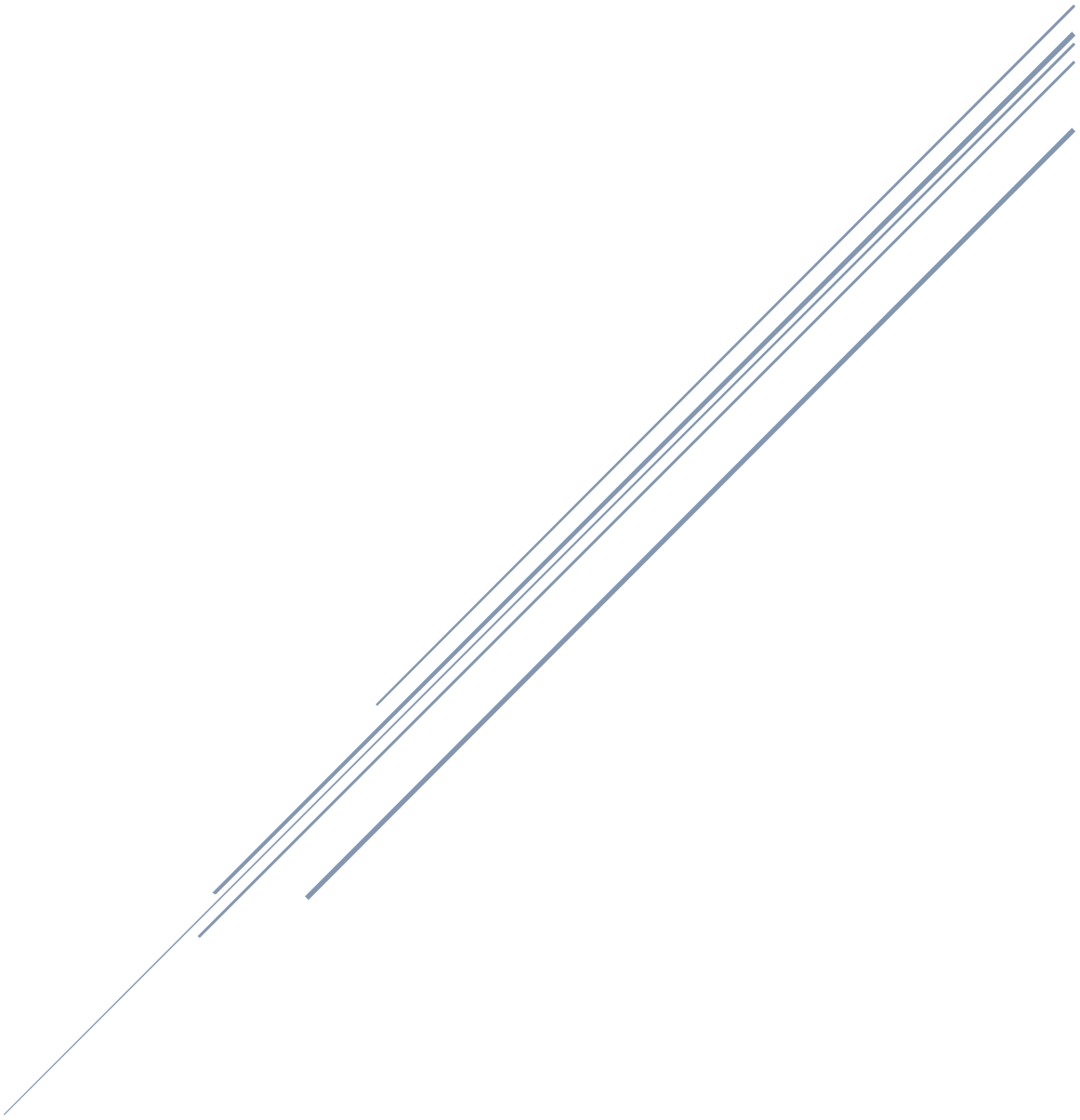
A mi madre por todas sus enseñanzas, consejos, cariño y amor que me ha brindado día a día sin algún límite en cada rubro de la vida, mismas que serán el fruto de su éxito y esfuerzo. Gracias madre porque me llena de orgullo ser tu hijo, gracias por ofrecerme tu cariño, comprensión, atención, desvelo, cuidados, amor y soporte para compartir el día de hoy mi logro más significativo junto a ti, TE AMO.

A mi hermana, por todo el apoyo incondicional y alientos, a ambas por compartir noches de desvelo, frustración y gloria a lo largo de mi vida personal y profesional.

A ti que me acompañaste en este largo recorrido y siempre apoyaste y enseñaste más de lo que imaginé.

Contenido

CAPÍTULO I. INTRODUCCIÓN



Capítulo I. Introducción

En la empresa consultora en seguridad informática en donde laboré es una empresa de consultoría con especialización de servicios de tecnologías de la información y seguridad informática, con especial presencia en los mercados de gobierno, financiero y telecomunicaciones, se contaba con una ideología enfocada en entender, analizar y solucionar los retos que se obtienen en cada proyecto con eficiencia para la obtención de resultados mediante su enfoque sistemático, mediante procesos alineados a los objetivos del negocio y mejora continua, mostrando disposición y actitud de servicio para la atención en la obtención y cumplimiento de los requerimientos solicitados por el cliente.

Para fortalecer la presencia de la empresa consultora en seguridad informática ante los mejores proyectos, los procesos que realizan, se encuentran regidos por los estándares de alta calidad reconocidos mundialmente, lo que genera la versatilidad de la empresa y brinda una diversidad de clientes leales, junto con una amplia gama de servicios y soluciones de ciberseguridad, protección, monitoreo y atención de incidentes de amenazas avanzadas en la red abierta, Deep Web, Darknet y seguridad de la información, lo que le permite tener múltiples proyectos con el mismo cliente.

I.1 Descripción de la empresa

La empresa Consultora en seguridad informática en la que laboré es una empresa de consultoría con alta especialización en Servicios de TI y de Seguridad de la Información, con especial presencia en los mercados de Gobierno, Financiero y de Telecomunicaciones.

Misión

“Proveer a las organizaciones y a las personas de soluciones de administración de riesgo y servicios de TI para brindar libertad en un entorno de riesgo digital, así como la optimización y eficiencia en la operación.”

Visión

“Ser la empresa especialista líder en servicios de seguridad de la información y servicios de TI, integrando las mejores prácticas a nivel internacional entregando soluciones de valor al negocio de nuestros clientes.”

I.2 Organigrama

Empresa Consultora en seguridad informática tiene una organización empresarial interna muy robusta, la cual permite la gestión y manejo de cada proceso con la revisión, procesamiento y validación de las áreas que se involucran en cada proyecto, gestionando y validando los procesos y resultados obtenidos en cada una de las fases que conforman, así como la determinación en la toma de decisiones para mejorar la productividad y efectividad de cada solución que se ofrece ante los clientes. En la siguiente imágen (**Véase ilustración 1**), podemos observar el árbol jerárquico por el que se conforma la estructura organizacional de la empresa consultora de seguridad informática en la que laboré.

Ilustración 1. Organigrama de Empresa Consultora en seguridad informática

a) Comité Ejecutivo

La función principal del comité ejecutivo es la elaboración, validación y aprobación de políticas que rigen al personal de la empresa consultora en seguridad informática, así como los procesos para los colaboradores de la empresa, la metodología de cada proceso que se lleve a cabo en el ciclo de vida que posea la información de interés para los proyectos realizados, el formato de los entregables y proyectos que se llevarán a cabo por cada departamento de la empresa.

b) Dirección General

El objetivo primordial es la búsqueda de clientes potenciales, así como la actualización de conocimientos de todo el equipo de trabajo, creando una metodología basada en la experiencia laboral, fomentando la investigación, organización y buenas prácticas a toda la organización.

c) Dirección de Control Interno

Tiene como principal enmienda el auditar los procesos de cada área de la empresa consultora en seguridad informática, mejorar y generar nuevas políticas internas de uso y documentación que eviten una penalización ante organismos de certificación como ISO (International Organization for Standardization).

d) Dirección de Finanzas

Su principal labor, es la generación de pagos a proveedores, así como el recibimiento, cobro y pago de facturas electrónicas; Pago de nómina y adquisición de bienes materiales para el uso del personal de la empresa consultora en seguridad informática.

e) Dirección de Administración

La función de este departamento es la gestión de recursos materiales y humanos, así como el seguimiento de proyectos, entregables y reportes de avances sobre proyectos. Una función que posee es la del seguimiento a la facturación y cobranza de los clientes de la empresa consultora en seguridad informática.

f) Dirección de Operaciones

Tiene como objetivo principal la generación y presentación de propuestas a las licitaciones en donde la empresa consultora en seguridad informática en la que he laborado tiene acceso. Además de la gestión de recursos humanos y materiales durante la realización del proyecto desde el inicio al cierre de este.

g) Dirección Comercial

Área de la empresa consultora en seguridad informática encargada de la promoción de los servicios a diversas entidades que realizan un manejo de información interna o externa de carácter sensible, generando nuevos clientes, nuevas visitas a empresas visitadas anteriormente o la participación en licitaciones para la obtención de nuevos proyectos.

h) Dirección de Seguridad Defensiva

Se encarga de la instalación y seguimiento de dispositivos dedicados a la seguridad perimetral, generando alertas y monitoreo en activos de diversos clientes.

i) Dirección de Seguridad Ofensiva

Es el área encargada de la generación de escaneos de vulnerabilidades para la obtención de información de los clientes que se analiza, generando la facilidad del enlistado y remediación de los riesgos potenciales de la organización. En esta área, he laborado hasta la actualidad y será el núcleo de mi experiencia profesional.

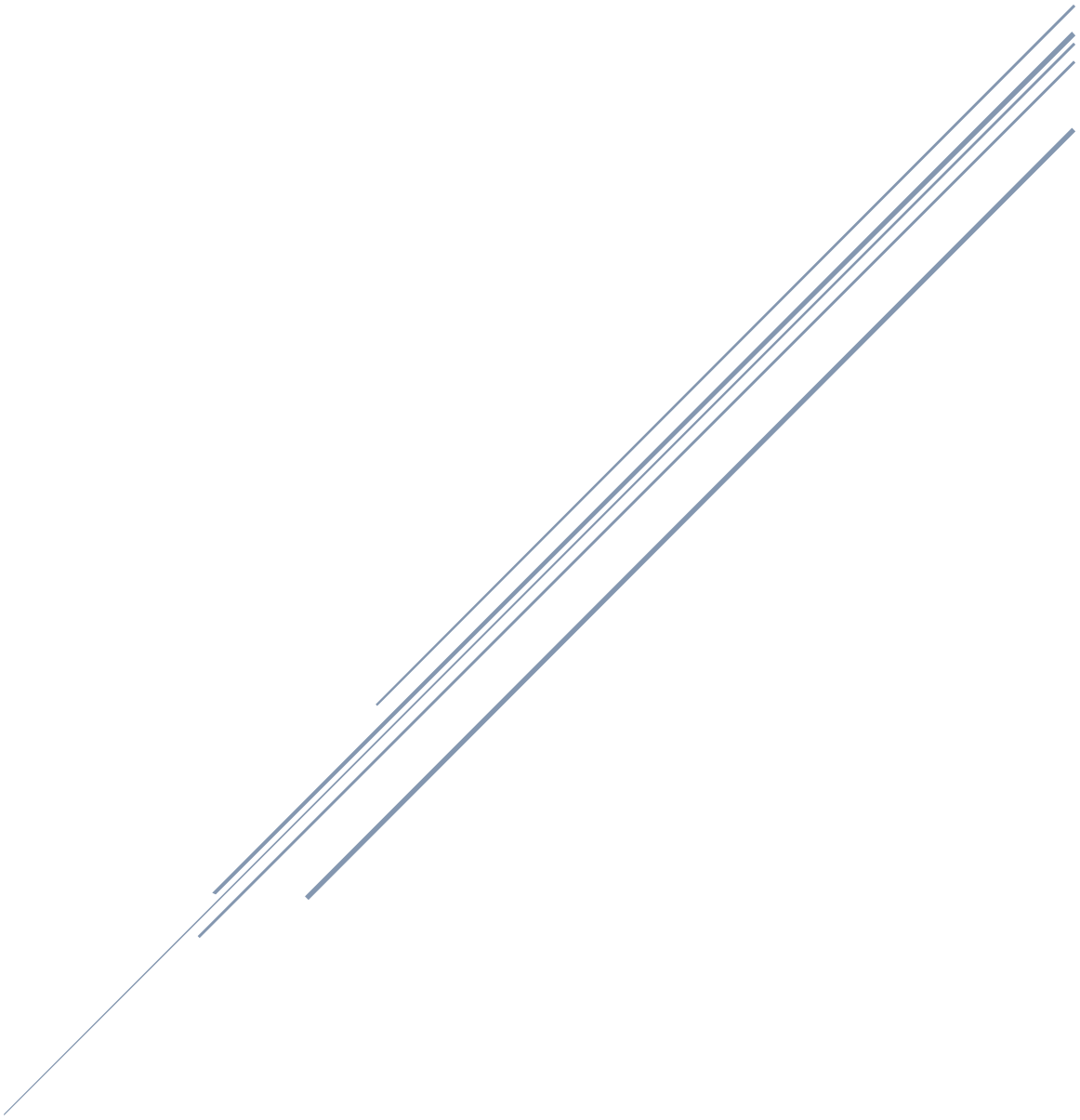
j) Dirección de Seguridad en Aplicativos

Departamento encargado de la elaboración de sistemas con diversos controles que proporcionarán al cliente un manejo más seguro de la información que fluya por aplicaciones elaboradas por los colaboradores de esta área.

k) Dirección de Investigación y Desarrollo.

Es el área que se dedica a la obtención de información actual de las tendencias de ataques en el mundo informático, así como de la preparación de cursos internos para la retroalimentar al personal.

CAPÍTULO II. ANTECEDENTES DE LA SEGURIDAD INFORMÁTICA



Capítulo II. Antecedentes de la seguridad informática

La seguridad de la información es el conjunto de procedimientos, estrategias, herramientas y procesos que permitan proporcionar un mayor control sobre la ***integridad***, la ***disponibilidad*** y la ***confidencialidad, autenticación, repudio y control de acceso*** de la información destinada para una entidad, institución o persona en los cuales se establece su base. Para el entendimiento superficial de la seguridad informática, a continuación, describiré cada aspecto de los seis tópicos en los que se basan sus principios:

a) Integridad

Se enfoca en la imposibilidad de que un agente externo o interno genere modificaciones de los datos sin ser descubierto. Lo que provee la integridad de los datos es la garantía de que nadie pueda acceder a la información ni modificarla sin poseer la autorización necesaria. Es requisito el verificar que los datos no sufran cambios no autorizados.

Para poder comprender la importancia de la integridad, debemos saber que la pérdida de integridad puede acabar en fraudes, decisiones erróneas o como paso previo a otro tipo de ataques.

b) Disponibilidad

Se refiere a la continuidad operativa de la entidad, sin interrupción en proveer los recursos a los que fue destinado ya que en el caso de no cumplir con esta premisa puede implicar en pérdida de productividad o credibilidad de la entidad. El sistema contiene información o proporciona servicios que deben estar disponibles a tiempo para satisfacer requisitos o evitar pérdidas importantes, como sistemas esenciales de seguridad y protección de la vida.

Un caso de pérdida de disponibilidad es el impacto en la producción y ventas que se verían reflejados en términos monetarios.

c) Confidencialidad

Se refiere a la protección de datos frente a la difusión no autorizada, la pérdida de confidencialidad puede resultar en problemas legales, pérdida del negocio o de credibilidad. El sistema contiene información que necesita protección contra la divulgación no autorizada, como información parcial de informes, información personal o información comercial patentada.

Un caso de riesgo por no cumplir con la confidencialidad de los datos es visible en los bancos, en donde compartir información de clientes, empleados e inversionistas puede llegar al quiebre del negocio por la fuga de inversionistas, demandas por circulación de información sensible y falta de validaciones por instituciones certificadoras a nivel nacional para llevar a cabo su función como institución bancaria.

d) Autenticación

Es la situación en la cual se puede verificar que un documento ha sido elaborado o pertenece a quien el documento dice. La autenticación de los sistemas informáticos, se realizan habitualmente mediante nombre, correo, sesión, identificador, usuario y algún otro rubro que tenga función de ser único y pertenezca a un solo usuario.

e) No repudio

El no repudio o irrenunciabilidad es un servicio de seguridad estrechamente relacionado con la autenticación y que permite probar la participación de las partes en una comunicación.

Existen 2 posibilidades:

- ✓ No repudio en origen: El emisor no puede negar el envío porque el destinatario tiene pruebas de que el receptor recibe una prueba infalsificable del envío.

- ✓ No repudio de destino: El receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción.

f) Control de acceso

Consiste en una serie de pasos a seguir para la verificación de una identidad (usuario, sistema, perfil, entre otros) en donde se solicita el acceso a una entidad autorizada quien verifica los requerimientos para obtener uno o más recursos.

Generalmente, un control de acceso está conformado por tres componentes principales:

1) **Mecanismo de autenticación**

Estos mecanismos pueden referirse a una contraseña, lector biométrico o cualquier otra entrada de información para que una entidad autentique la información con una base de datos o archivo de información donde encuentre la coincidencia de la información ingresada con la información almacenada.

2) **Mecanismo de autorización**

Es un intermediario entre el mecanismo de autenticación y el mecanismo de trazabilidad ya que verifica los permisos necesarios para que una entidad ingrese o no a un recurso inclusive si está correctamente autenticado.

3) **Mecanismo de trazabilidad**

Es quien genera el panorama completo de acción para una entidad o usuario, ayudando así a la identificación de acciones realizadas dentro de un sistema.

II.1 ¿Qué es lo que desea proteger la seguridad informática?

En un sistema informático lo que queremos proteger son sus activos, es decir, los recursos que forman parte del sistema y que podemos agrupar en:

- ✓ Hardware: Elementos físicos
- ✓ Software: Elementos lógicos
- ✓ Datos: Información manejada por el hardware y el software
- ✓ Otros: Capital Humano, Infraestructuras, entre otros.

De los cuales, los más críticos son los datos, el hardware y el software ya que los datos que están almacenados en el hardware y que son procesados por las aplicaciones software. Teniendo como el activo más valioso a la información de la empresa, pues en ella se puede transportar información sensible para trabajadores, clientes e inversionistas; lo que podría provocar la desaparición del negocio y posiblemente problemas legales.

Una medida muy concurrida para el cuidado de los datos es una política de respaldo de seguridad robusta, que sea capaz de restablecer los datos hasta un punto cercano al cual se detectó la pérdida. Esto puede suponer para la empresa, por ejemplo, la dificultad o imposibilidad de reponer dichos datos con lo que se consume el tiempo y dinero, sabiendo que es el objetivo de transformar un dato a un activo de interés para la medida de métricas o toma de decisiones (véase Ilustración 2).

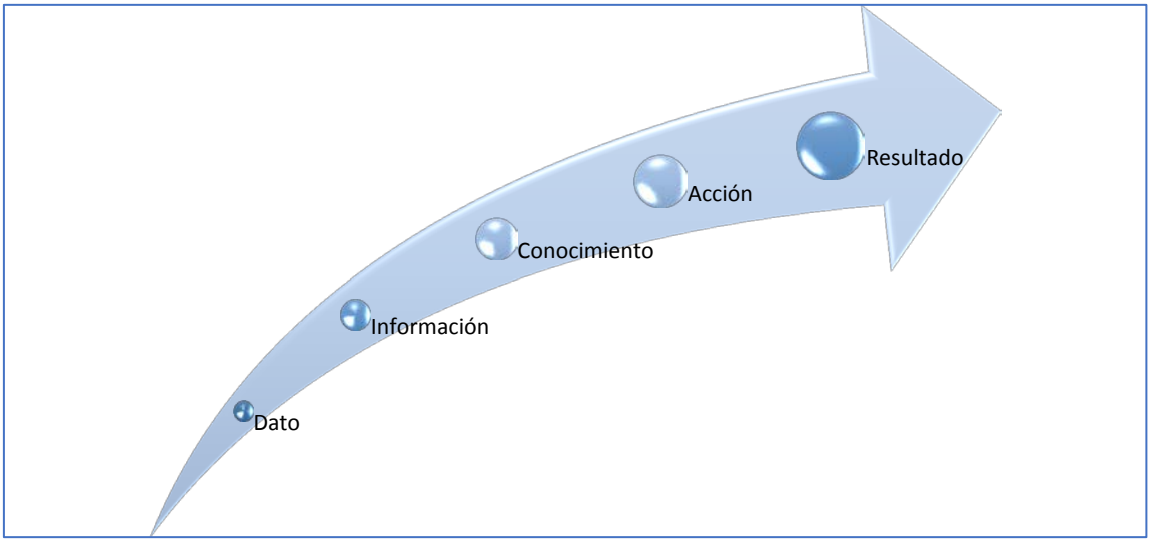


Ilustración 2. Proceso de conversión de un dato a un resultado determinado

II.2 Tipos de vulnerabilidades informáticas

Una vulnerabilidad es un fallo o debilidad de un activo o grupo de activos que posee una anomalía en su funcionamiento, presentando diferentes tipos de riesgos que elevan la probabilidad de ser explotada por una o más amenazas que permiten:

- Ejecutar comandos como otro usuario.
- Acceder a datos contrarios a las restricciones de acceso especificados para estos datos.
- A un usuario, hacerse pasar por una persona con permisos.
- Realizar una denegación de servicio.
- La consulta o manipulación de un activo.

Comúnmente, se pueden clasificar las vulnerabilidades informáticas de la siguiente manera:

i. Vulnerabilidad de día cero (0-day).

Una nueva vulnerabilidad para la cual no se crearon actualizaciones o revisiones, y que se emplea para llevar a cabo un ataque. El nombre 0-day (día cero) se debe a que aún no existe ninguna actualización para mitigar el aprovechamiento de la vulnerabilidad.

ii. Vulnerabilidades de desbordamiento de buffer.

Se produce cuando un programa no controla la cantidad de datos que se copian en la entrada de datos llamada búffer, de forma que si esa cantidad es superior a la capacidad del buffer los bytes sobrantes se almacenan en zonas de memoria adyacentes, sobrescribiendo su contenido original.

iii. Vulnerabilidades de condición de carrera (race condition).

La condición de carrera se da principalmente cuando varios procesos acceden al mismo tiempo a un recurso compartido, por ejemplo, una variable, cambiando su estado y obteniendo de esta forma un valor no esperado de la misma.

iv. Vulnerabilidades de error de formato de cadena (format string bugs).

La principal causa de los errores de cadena de formato es aceptar sin validar la entrada de datos proporcionada por el usuario. Un ataque puede conducir de manera inmediata a la ejecución de código arbitrario y a revelación de información.

v. Vulnerabilidades de Cross Site Scripting (XSS)

Abarcaban cualquier ataque que permitiera ejecutar scripts como VBScript o **JavaScript**, en el contexto de otro sitio web. Estos errores se pueden encontrar en cualquier aplicación que tenga como objetivo final presentar la información en un navegador web.

Un uso de esta vulnerabilidad es hacer phishing. La víctima ve en la barra de direcciones un sitio, pero realmente está en otro. La víctima introduce su contraseña y se la envía al atacante.

vi. Vulnerabilidades de Inyección SQL (SQL Injection)

Una inyección SQL se produce cuando, de alguna manera, se inserta o "inyecta" código SQL invasor dentro del código SQL programado, a fin de alterar el funcionamiento normal del programa y lograr así que se ejecute la porción de código "invasor" incrustado, en la base de datos.

vii. Vulnerabilidades de denegación del servicio (DDoS)

La denegación de servicio provoca que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos informáticos del sistema de la víctima.

viii. Vulnerabilidades de suplantación de identidad (Phishing)

Las ventanas engañosas son aquellas que dicen que eres el ganador de tal o cual cosa, lo cual es mentira y lo único que quieren es que des información. Hay otro tipo de ventanas que, si las sigues, obtienen datos del ordenador para luego realizar un ataque o extorsión.

II.4 ¿Qué es un hacker?

La tecnología ha dejado de ser un lujo o privilegio en todo el mundo, su uso se ha convertido en un elemento fundamental en el ámbito personal y empresarial. En un mundo tan activo y globalizado, las empresas deben ser rápidas y eficientes con todos sus recursos y procesos en los cuales, la tecnología ha llegado para resolver los problemas y eliminar las barreras de las organizaciones a través de sistemas innovadores y adaptables a las necesidades de cada una. Las empresas en vías de crecimiento deben luchar cada día por ir de la mano con los avances tecnológicos y adaptarse a ellos, con el fin de acelerar sus procesos y por supuesto, mantener competitividad en el mercado en los principales aspectos empresariales como lo son los procesos óptimos, en los que se comprenden:

- ✓ Mayor productividad
- ✓ Adiós a las barreras de comunicación
- ✓ Competitividad en el mercado
- ✓ Mejor toma de decisiones

Los analistas de errores y vulnerabilidades en los procesos antes mencionados y en los sistemas informáticos que se han convertido en los últimos años en la alternativa de escape, sin un gran corporativo, entidad bancaria o institución gubernamental que no disponga de un grupo de expertos de la seguridad que se encuentren dispuestos a sumarse a sus filas en caso de un incidente de seguridad. Normalmente, esta clase de expertos, buscan fallos en los sistemas que les proporcione una entrada para obtener algún recurso y poder obtener algo a cambio por dicho elemento que suele ser muy preciado por las empresas. Dichos expertos, por lo común se conocen como "hackers", siendo así un grupo muy temido por cualquier organización, pero el término ha sido modificado en diversas ocasiones, quedando una transformación de acuerdo con la época en donde se ha descrito (véase Ilustración 3).

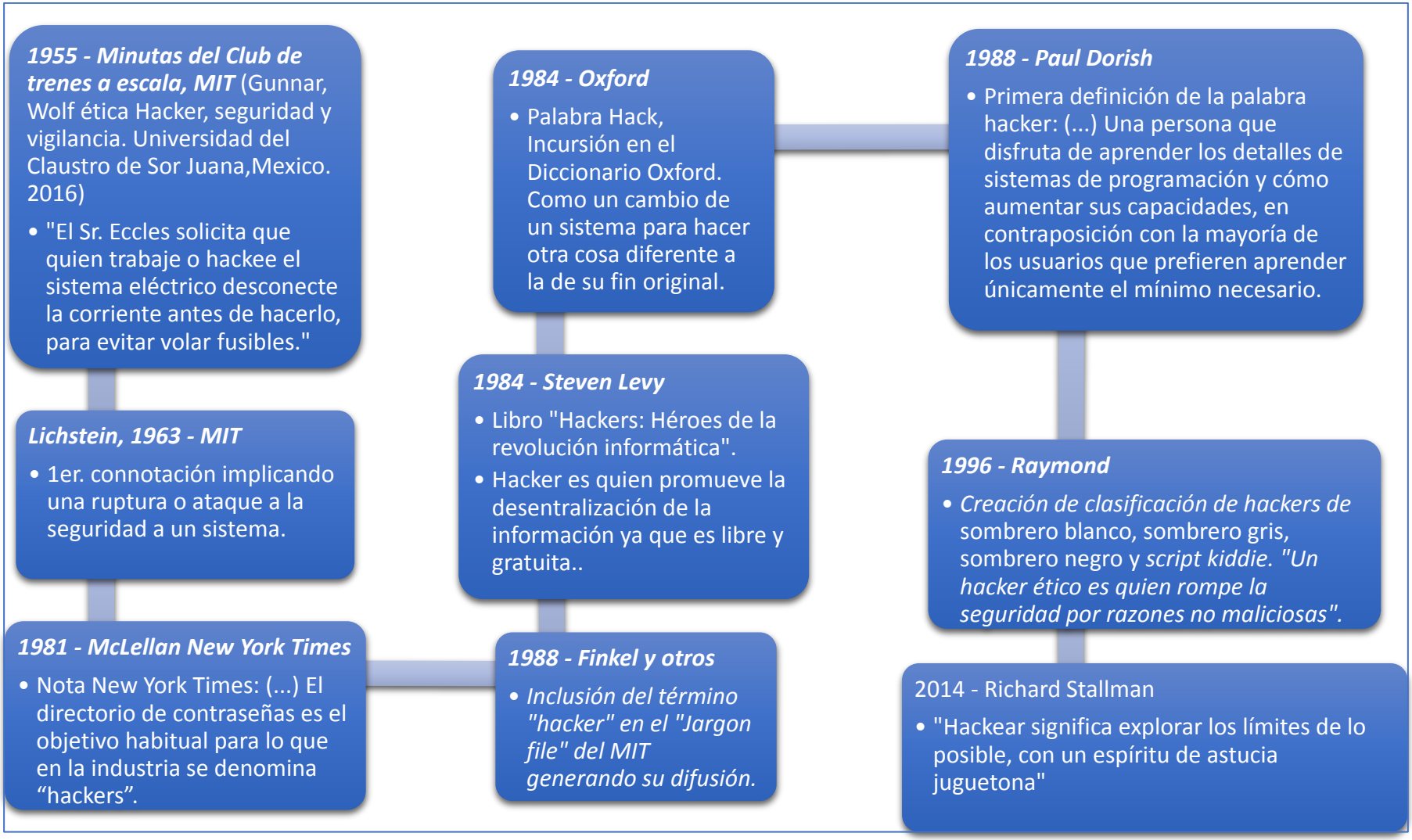


Ilustración 3. Evolución del término hacker.

II.5 Expertos de la seguridad informática

Hoy en día, para las organizaciones e instituciones privadas y del sector gobierno es de vital importancia poseer sistemas e infraestructuras informáticas que posean políticas y medidas de seguridad adecuadas, con el fin de garantizar la disponibilidad y sostenibilidad de sus actividades, eso precisamente, es lo que se pretende con la implantación de seguridad en sistemas informáticos.

Para cualquier tipo de empresa, es imprescindible disponer de un plan adecuado de seguridad para sus redes informáticas, que garantice desde la privacidad de los datos hasta la integridad en las transacciones de información, pasando por el control de acceso, los protocolos de comunicación, las transferencias de datos y otros tipos de operaciones sensibles. Para estas tareas, se puede llegar a hacer una búsqueda de una persona con las capacidades suficientes, pero dentro de un mundo informático, existen una gran variedad de individuos que se pueden categorizar dependiendo de sus acciones e intenciones, entre ellos y dependiendo de la gravedad, objetivo o urgencia de la resolución o atención de las tareas, podemos definir tres categorías principalmente:

Categoría 1. Whitehats o hackers éticos

Son profesionales dedicados a la búsqueda y solución de vulnerabilidades en sistemas empresariales, gubernamentales y particulares. Estas personas suelen trabajar para las empresas de informática bajo un contrato que los respalda en sus actividades y evitando problemas legales debido a dichas acciones. Dentro de este grupo podemos englobar a dos subgrupos:

- **Bluehat hackers (“sombreros azules”).** Generalmente son consultores o profesionales externos de seguridad dedicados a las pruebas de seguridad de un software o hardware antes de su lanzamiento oficial y salida al mercado, para intentar exponer las vulnerabilidades existentes, paralelamente al trabajo realizado por el propio grupo interno de la empresa y generando una tercera opinión.

- **Red Hat hackers (“sombreros rojos”).** Este tipo de hacker se caracteriza principalmente por utilizar, promover y mejorar el software libre.

Categoría 2. Greyhat hackers.

Son un grupo de personas que trabajan indistintamente para firmas de seguridad como para organizaciones criminales, periódicamente integran trabajo con sus

necesidades, generando la necesidad de la obtención de más ingresos y en ocasiones, se sigue la línea de todo un proceso ético, puede llamarse un intermedio entre un whiteHat y un blackhat.

Categoría 3. Blackhats

Son personas dedicadas a utilizar (de forma profesional o amateur) sus conocimientos para actividades delictivas y sacar un provecho económico para el cubrimiento total de sus necesidades, gusto y ambiciones sin ninguna consideración hacia sus necesidades.

II.6 La otra cara de la profesionalización: el mercado negro y la ciberdelincuencia organizada

Cuando el mercado no puede absorber en empresas lícitas el conocimiento de las personas con talento hacker, pueden aparecer otras organizaciones que intenten rentabilizar sus habilidades en otras áreas orientadas a la criminalidad. Se trata de crackers, spammers, scammers, phishers organizados que, como las mafias, se dedican al lucro propio de forma profesional. Existen tantos tipos como actividades delictivas en el mundo digital:

I. **Phreakers.** Equivalente en sistemas telefónicos al cracker, se le supone amplios conocimientos sobre las tecnologías y mecanismos que intervienen en las comunicaciones digitales y analógicas, siendo capaces de interceptarlas y tomar control del sistema para su propio beneficio. Para ejemplificar, su apogeo fue en los años 70 y 80 con la creación y distribución de la bluebox y posterior blackbox. Se trataba de pequeños dispositivos analógicos-digitales que permitían realizar llamadas gratuitas desde los antiguos sistemas de telefonía.

II. **Phishers.** Dedicados al fraude bancario, diseñan, habilitan y gestionan sitios falsos de webs bancarias o sistemas de pago, principalmente para intentar engañar a los usuarios y conseguir sus credenciales de sus cuentas o de las tarjetas de crédito. Sus delitos se pueden observar de manera diaria desde cargos no identificados a tarjetas de cuentahabientes a compras electrónicas.

III. **Scammers.** Dedicados a todo tipo de estafas en la red, ya sea vendiendo productos fraudulentos, simulando la prestación de servicios ficticios, etc. Una estafa particularmente persistente tiene su origen en Nigeria y hace referencia a todo ese compendio de correos electrónicos ofreciendo herencias o depósitos millonarios, que necesitan ser retirados del país rápidamente por encontrarse en una situación límite. Piden ayuda a la víctima para custodiar esa gran suma de dinero a cambio de un porcentaje. De las estafas realizadas por esta actividad son los correos electrónicos describiendo una herencia vacante que la víctima adquirirá, una cuenta bancaria abandonada, una lotería que la víctima ha ganado, entre otras en donde solo obtenían los depósitos de las personas sin nada a cambio.

IV. **Spammers.** Quienes generan y distribuyen correo basura. El spam supone gran parte de tráfico de correos electrónicos a nivel mundial y una de las mayores molestias para los usuarios. Aunque a simple vista inofensivo, en realidad se trata de una herramienta esencial para phishers y scammers

que la utilizan como vehículo para conducir a sus víctimas a sitios fraudulentos o infecciosos. Hoy en día podemos observar este tipo de actividades en la bandeja de spam de nuestros correos personales de manera diaria, sobre productos o servicios generales que pueden esperar solo ingresar a las ligas que contienen para obtener información personal o de valor para estos atacantes.

V. **Skimmers y carders.** Son aquellos sujetos y mafias encargados de la clonación de tarjetas bancarias. Sus objetivos suelen ser clientes en tiendas o restaurantes en colaboración con algún trabajador del local que obtenga acceso a la tarjeta en el momento del paso por el terminal o cualquier usuario de un cajero que haya sido modificado para copiar las bandas magnéticas. Todos ellos se dedicarían al skimming (manipulación de los dispositivos que leen las tarjetas para poder extraer sus datos y clonarlas), siendo la función del carding comprobar que esos datos siguen siendo válidos para su distribución y uso.

VI. **Crackers.** Un cracker puede haberse o no formado en la cultura y conocimientos propios del movimiento, pero el hecho de utilizarlos en su propio beneficio dañando a los demás, supone por sí solo un hecho diferenciador que lo aleja del verdadero hacking. Aunque se trata un subtipo de hacking, no es considerado como un verdadero hacker por las connotaciones peyorativas que posee, y por alejarse de filosofía hacker. Se consideran en esta clasificación tanto los atacantes, como los hackers dedicados a crear “cracks” (pequeños programas que permiten eludir la licencia de software de pago).

VII. **Lammers**. Persona generalmente con pocos conocimientos técnicos que los utiliza para vanagloriarse y hacerse pasar por un verdadero hacker.

VIII. **Scriptkiddies**. Aprendices que tampoco llegan a mejorar en sus conocimientos y se dedican a ejecutar guías paso a paso o utilizar pequeños conjuntos de herramientas realizadas por terceros. Su objetivo es conseguir algún tipo de reconocimiento dentro del movimiento o simplemente realizar ***defacements*** denegaciones de servicio impidiendo el acceso a las mismas.

IX. **Piratería.** Se define como la acción de distribuir contenido digital protegido por derechos de propiedad intelectual (copyright) con el objetivo de conseguir una remuneración económica, bien por la distribución y/o venta, o bien por ingresos a través de publicidad.

X. **Hacktivismo.** Mención especial merece este término que hace referencia a las actuaciones de determinados hackers para defender, dar a conocer o tomar conciencia sobre hechos, conflictos o abusos políticos. Aunque

pueda parecer íntimamente relacionado con el movimiento Anonymous no lo están. Estos sí pueden ser grupos de hackers, profesionales u expertos que protestan de una determinada manera en el mundo digital para demostrar su punto de vista (político o social). Los primeros ciudadanos del mundo que están asociados públicamente en este tipo de movimientos son Julian Assange y Edward Snowden, pues son los primeros ciudadanos de la red quienes son acusados de mal uso del hacktivismo.

II.7 La profesionalización de un hacker: El hacking ético

Como en cualquier otra actividad, puede llegar un momento en el que se generan necesidades tecnológicas en empresas y gobierno, por lo cual deben ser atendidas. Es por ello por lo que el mundo del hacking ha evolucionado, profesionalizándose en todas sus etapas y en todos los ámbitos sociales, empresariales y legales.

El hacking ético engloba todos aquellos servicios prestados para la seguridad de las instituciones tanto por hackers como por consultores y expertos en seguridad. Principalmente, estos servicios están orientados a la simulación de intrusiones reales en los sistemas empresariales para llevar a cabo un análisis y evaluación de las vulnerabilidades para que, posteriormente la empresa las solucione y así evite tener una incidencia de seguridad como una posible intrusión en sus sistemas.

Los ethical hackers son expertos que realizan una serie de medidas para determinar la vulnerabilidad de un sistema. A esta práctica normalmente se le conoce como pentest (penetration test) o test de intrusión, en las cuales, nos pueden ayudar en diversas actividades las cuales se enlistan a continuación:

a) Evaluar los activos a través de la identificación de debilidades provocadas por una mala configuración de las aplicaciones, falta de mantenimiento o mala administración propia de los activos o de otros componentes de la red.

b) Analizar y categorizar las debilidades explotables, con base al impacto potencial y la posibilidad de que la amenaza se convierta en realidad y genere un impacto en la disponibilidad, integridad y confidencialidad de los recursos de una empresa.

c) Proveer recomendaciones con base en las prioridades de la organización para mitigar y eliminar las vulnerabilidades y así reducir el riesgo de ocurrencia de un evento desfavorable, aunque haciendo hincapié en que un sistema jamás será 100% seguro. Para ello, se sigue una serie de pruebas, usadas también por los atacantes (recopilación de información, descripción de la red, exploración de los sistemas, extracción de información, acceso no autorizado a información sensible o crítica, auditoría de las aplicaciones web), pero con la diferencia de haber sido consensuadas previamente con los responsables del sistema objetivo.

La búsqueda de vulnerabilidades en el software, que llevan a cabo los profesionales encargados de detectar activa o pasivamente fallos en el software.

Dependiendo de si el fallo descubierto se comunica de forma responsable a los fabricantes se hablará de una "divulgación completa" o "divulgación responsable".

En el primer caso, se hacen públicos todos los datos técnicos del error, sin avisar previamente al fabricante. Esto puede llegar a considerarse una irresponsabilidad y ser calificado de "vandalismo". En el caso del “divulgación reponsable”, se coordina con los responsables del programa una solución para así hacer público el fallo cuando ya existe un parche que permita proteger a sus clientes.

II.8 ¿Qué es un consultor de seguridad informática?

Un consultor de seguridad informática es aquel individuo que posee conocimientos sólidos de seguridad en redes de datos para proveer un asesoramiento y supervisión sobre las medidas de seguridad necesarias para brindar la mayor protección de manera efectiva para los activos de una empresa o cliente. Dicho asesoramiento tiene su base en el conocimiento, investigación y experiencia adquirida, mismos que son invertidos en la evaluación de amenazas potenciales para los bienes de una empresa o cliente, proponiendo acciones preventivas con desarrollo de políticas preventivas y planes de contingencia, con preparación para cualquier tipo de **incidencia informática**.

El consultor de seguridad informática es un término simple, pero abarca un sentido más amplio y polifacético dado que atiende una diversidad de temas ya que éste debe conocer no sólo acerca de su materia, sino que, también, tendrá conocimientos de las demás ramas de la seguridad (electrónica, industrial, bancaria, informática, aeroportuaria, etc.).

El consultor de seguridad ha podido obtener su experiencia desde su formación académica mediante estudios universitarios o por haber desarrollado la profesión para la cual es citado, además de ser una persona con experiencia, con acreditaciones y capacidades probadas, necesarias para cumplir con una tarea que una persona o empresa pueda necesitar sobre un tema específico.

Aunque no siempre es necesario poseer una formación académica, ya que ha habido ocasiones en donde el consultor llega a un puesto por toda su experiencia y pericia que ha desarrollado por sí mismo aún después de haber pasado un juicio legal o cumplir una condena previa.

Es la persona que tiene la capacidad de resolver problemas porque tiene la pericia y los conocimientos técnicos basados en la experiencia de la práctica cotidiana de la actividad.

Las personas que se dedican a la consultoría de seguridad poseen la facilidad de creación de un perfil exclusivo para los profesionales del mismo ramo, ya que la seguridad informática es una disciplina que a creciendo muy rápidamente, por lo que cada vez se requiere de individuos con mayores capacidades y control de diversos temas que comprende el rol de consultor de seguridad, como los cuales desde mi punto de vista son:

- Programación
- Estándares y protocolos
- Redes de datos
- Infraestructura de redes de datos
- Políticas
- Documentación
- Escaneo de puertos
- Escaneo de vulnerabilidades
- Explotación de vulnerabilidades
- Ética profesional

II.9 Funciones principales de un consultor de seguridad informática

A continuación, las funciones más comunes de un consultor de Seguridad informática:

- **Establecer protocolos y políticas de seguridad, además de diseñar planes de seguridad para proteger los activos del cliente**

  - ✓ Crear un conjunto de reglas y estándares de seguridad.
  - ✓ Diseñar políticas de uso para proteger los activos del cliente.
  - ✓ Implementar medidas de seguridad, brindando la supervisión técnica que sea necesaria.

- **Reunirse con los clientes**

  - ✓ Analizar los bienes del cliente e identificar las medidas de seguridad necesarias.
  - ✓ Capacitar sobre protocolos y medidas de seguridad.
  - ✓ Identificar las amenazas potenciales de seguridad.
  - ✓ Seleccionar las medidas de seguridad que sean óptimas.
  - ✓ Revisión de incidentes y eventos de seguridad.

- **Ejecutar pruebas de vulnerabilidad**

  - ✓ Realizar pruebas de riesgos.
  - ✓ Analizar las violaciones potenciales.
  - ✓ Diseñar un plan para eliminar la mayor cantidad de riesgos.
  - ✓ Elaborar y presentar informes basados en los descubrimientos.

- **Estar al corriente con los últimos estándares de seguridad**

  - ✓ Conocer sobre los nuevos sistemas y herramientas de seguridad y tecnología del mercado.

- **Coordinar un equipo de especialistas de seguridad**

  - ✓ Contratar y entrenar a los nuevos miembros del equipo.
  - ✓ Asignar tareas a cada miembro del equipo.
  - ✓ Crear un plan de monitoreo de vulnerabilidades constante.
  - ✓ Coordinar y supervisar las actividades del equipo.
  - ✓ Evaluar las situaciones de emergencia y coordinar una respuesta apropiada.

II.10 Labores diarias de un consultor de seguridad informática

Un consultor de seguridad, además de cumplir con las actividades mencionadas anteriormente, se debe tener un cumplimiento por día de las actividades que se describen y muestran en la siguiente figura (**véase Ilustración 4**):

- Inspeccionar los bienes de los clientes para determinar el nivel de seguridad requerido.

- Diseñar protocolos, planes y sistemas de seguridad.

- Implementar medidas de seguridad y establecer políticas para los clientes.

- Coordinar reuniones con el equipo de seguridad y asignar tareas a los miembros del equipo.

- Reunirse con los clientes para explicarles las medidas de seguridad y para brindar asesoría en sistemas de seguridad.

- Realizar pruebas de seguridad, escaneo de vulnerabilidades, así como analizar y reportar los resultados obtenidos.

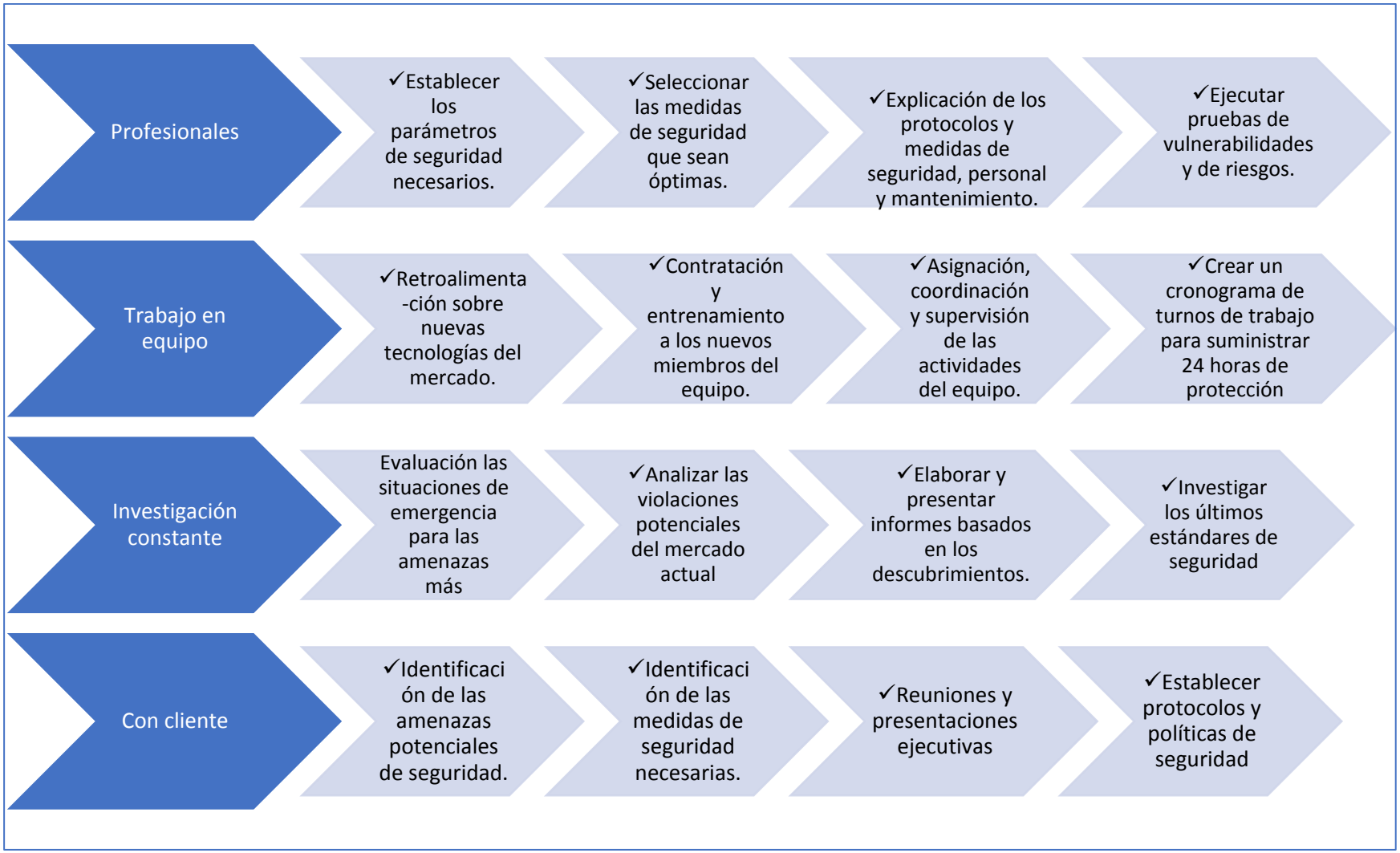


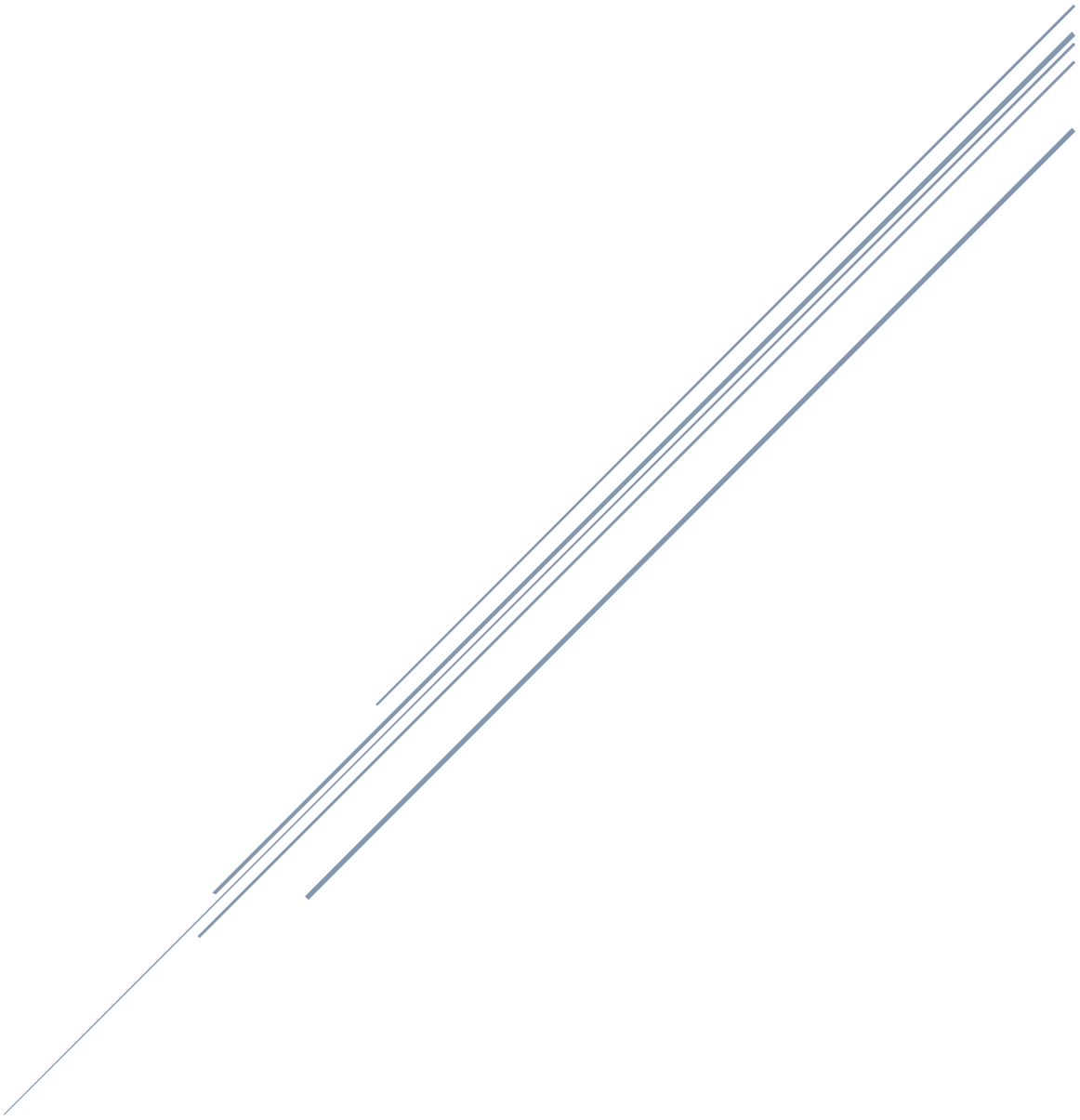
Ilustración 4. Funciones principales de un consultor

II.11 Capacitación para un consultor de seguridad

La seguridad de la información tiene una sólida base y respaldo de Instituciones de confianza y/o avaladas para proporcionar instrucción y certificación sobre temas de seguridad informática, las cuales hacen uso de: estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos en el manejo de la infraestructura computacional e información contenida para los clientes o visitantes en el medio electrónico. Algunas de las instituciones más reconocidas que cuentan con la validez internacional para crear cursos, certificaciones y boletines acerca de amenazas se muestran en la siguiente tabla:

Entidades certificadoras en seguridad informática	
SANS INSTITUTE	Es la fuente de capacitación en seguridad de la información más confiable y de lejos la más grande del mundo. Ofrece capacitación a través de varios métodos de capacitación: en vivo, virtual, estilo de aula, en línea a su propio ritmo, transmisión por Internet con instrucción en vivo, estudio guiado con un mentor local o privado y en el ambiente laboral; con certificaciones en seguridad cibernética, seguridad de red, análisis forense, liderazgo en seguridad y seguridad de aplicaciones.
ISC²	Es una asociación de membresía internacional sin fines de lucro para líderes de seguridad de la información. Cuenta con el compromiso de ayudar a sus miembros a aprender, crecer y prosperar. Con más de 130,000 miembros certificados, fortaleciendo a los profesionales que tocan todos los aspectos de la seguridad de la información.
OFFENSIVE SECURITY	Certificaciones y cursos de capacitación en seguridad de pruebas de penetración más realistas de la industria. Impartido por los desarrolladores de la distribución profesional de Kali Linux.
ISACA	ISACA® (isaca.org) ayuda a los profesionales globales a liderar, adaptar y asegurar la confianza en un mundo digital en evolución ofreciendo conocimiento, estándares, relaciones, acreditación y desarrollo de carrera innovadores y de primera clase. Establecida en 1969, ISACA es una asociación global sin ánimo de lucro de 140 000 profesionales en 180 países.

CAPÍTULO III. METODOLOGÍA



Capítulo III. Metodología

Una metodología es una serie de pasos a seguir para realizar una evaluación de la seguridad de un sistema u organización, simulando un ataque real y el escenario de recuperación que llevaría a cabo cualquier ciberdelincuente que pretendiera obtener el control del sistema, realizar manipulación de la información o robarla.

Para llevar a cabo las pruebas realizadas en diferentes instituciones, se siguió una metodología definida por el departamento de seguridad ofensiva de la empresa consultora en seguridad informática en donde realicé pruebas de penetración llamada PTES.

El proyecto PTES (Penetration Testing Execution Standard) surgió a principios del año 2009, pretendiendo unir esfuerzos de analistas y expertos de la seguridad informática. Este estándar se encuentra en la versión 1.0 y fue diseñado para ofrecer a las empresas y proveedores de servicios un lenguaje y enfoque común para realizar pruebas de penetración.

Ilustración 5. Logo metodología PTES

Estas fases cubren todo lo relacionado con una prueba de penetración, desde la comunicación inicial y el razonamiento detrás de un pentest, pasando por la recopilación de inteligencia y las fases de modelado de amenazas donde los evaluadores trabajan detrás de escena para obtener una mejor comprensión de la organización probada, a través de investigaciones de vulnerabilidad. explotación y post-explotación, donde la experiencia técnica de seguridad de los evaluadores viene a comprobarse y se combina con la comprensión comercial del compromiso, y finalmente a la presentación de informes, que captura todo el proceso, de

manera que tenga sentido para el cliente y proporcione mayor valor para su negocio.

Esta metodología consta de siete fases, las cuales se mencionarán a continuación: (ver ilustración 6)

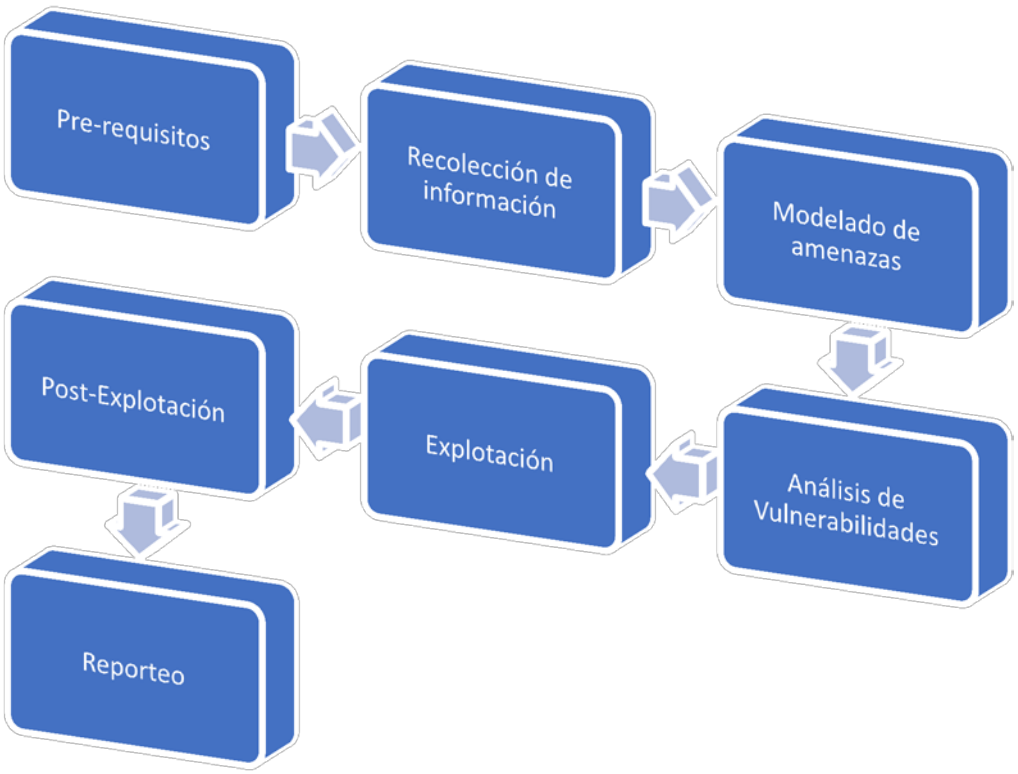


Ilustración 6. Fases metodología PTES

- ✓ **Contacto previo a las pruebas**

El objetivo de esta sección de la metodología PTES es presentar y explicar las herramientas y técnicas disponibles que ayudan en un paso previo al compromiso exitoso de una prueba de penetración. La información de esta sección es el resultado de los muchos años de experiencia combinada de algunos de los probadores de penetración más exitosos del mundo.

- ✓ **Recopilación de Inteligencia**

Esta sección define las actividades de recopilación de inteligencia de una prueba de penetración. El propósito de esta fase es proporcionar un estándar diseñado

específicamente para que el especialista en seguridad realice un reconocimiento contra un objetivo determinado. La fase detalla el proceso de pensamiento y los objetivos del reconocimiento de las pruebas de penetración, y cuando se usa adecuadamente, ayuda al lector a producir un vector de ataque altamente estratégico para vulnerar a su objetivo.

- ✓ **Modelado de amenazas**

Esta sección define un enfoque de modelado de amenazas como se requiere para una ejecución correcta de una prueba de penetración. El estándar no utiliza un modelo específico, sino que requiere que el modelo utilizado sea consistente en términos de su representación de amenazas, sus capacidades, sus calificaciones según la organización que se está probando y la capacidad de aplicarse repetidamente a pruebas futuras con el mismo resultado.

- ✓ **Análisis de vulnerabilidad**

La prueba de vulnerabilidad es el proceso de descubrir fallas en sistemas y aplicaciones que pueden ser aprovechadas por un atacante. Estos defectos pueden variar desde la configuración incorrecta del host y del servicio, hasta el diseño de aplicaciones inseguras. Aunque el proceso utilizado para buscar fallas varía y depende en gran medida del componente particular que se está probando, algunos principios clave se aplican al proceso.

- ✓ **Explotación**

La fase de explotación de una prueba de penetración se centra únicamente en establecer el acceso a un sistema o recurso al eludir las restricciones de seguridad. Si la fase anterior, el análisis de vulnerabilidad se realizó correctamente, esta fase debe estar bien planificada y una huelga de precisión. El objetivo principal es identificar el punto de entrada principal en la organización e identificar los activos objetivo de alto valor.

Si la fase de análisis de vulnerabilidad se completó correctamente, se debería haber cumplido una lista de objetivos de alto valor. En última instancia, el vector de ataque debe tener en cuenta la probabilidad de éxito y el mayor impacto en la organización.

- ✓ **Explotación posterior**

El objetivo de la fase posterior a la explotación es determinar el valor de la máquina comprometida y mantener el control de la máquina para su uso posterior. El valor de la máquina está determinado por la sensibilidad de los datos almacenados en él y la utilidad de las máquinas para comprometer aún más la red. Los métodos descritos en esta fase están destinados a ayudar al probador a identificar y documentar datos confidenciales, identificar ajustes de configuración, canales de comunicación y relaciones con otros dispositivos de red que pueden usarse para obtener acceso adicional a la red, y configurar uno o más métodos de acceder a la máquina en un momento posterior.

- ✓ **Reporteo**

Este documento está destinado a definir los criterios básicos para los informes de pruebas de penetración. Si bien se recomienda enfáticamente utilizar su propio formato personalizado y de marca, lo siguiente debe proporcionar una comprensión de alto nivel de los elementos requeridos dentro de un informe, así como una estructura para que el informe proporcione valor al lector.

Dado que el estándar no proporciona ninguna guía técnica en cuanto a cómo ejecutar una prueba de penetración de manera correcta, he creado una guía técnica para acompañar el estándar en sí mismo, separando las pruebas en parte ***externa*** e ***interna*** como se muestra a continuación.

III.*1* Pruebas de penetración externa

Es una evaluación crítica, sistemática y detallada de redes informáticas desde una red externa a la que se está tratando de ingresar en una prueba de penetración. Es un procedimiento que se realiza por parte de un consultor de seguridad de una empresa consultora de seguridad informática como en la que me encuentro laborando, y en el cual se utilizan técnicas establecidas con el objeto de emitir informes y formular sugerencias para el mejoramiento de la seguridad.

La prueba de penetración externa es la evaluación externa del entorno de seguridad de una empresa desde la perspectiva de un hacker a través de internet o de alguien que no tiene acceso a los recursos informáticos. Permite identificar y solucionar vulnerabilidades informáticas antes que los hackers puedan comprometer la información confidencial. El servicio de evaluación externa debe cubrir todos los nuevos tipos de ataques externos y no sólo probar los ataques convencionales si no, tartar de encontrar vulnerabilidades recientes o de día cero.

Los pasos por seguir de una prueba de penetración externa se muestran a continuación: (**véase la Ilustración 7**).

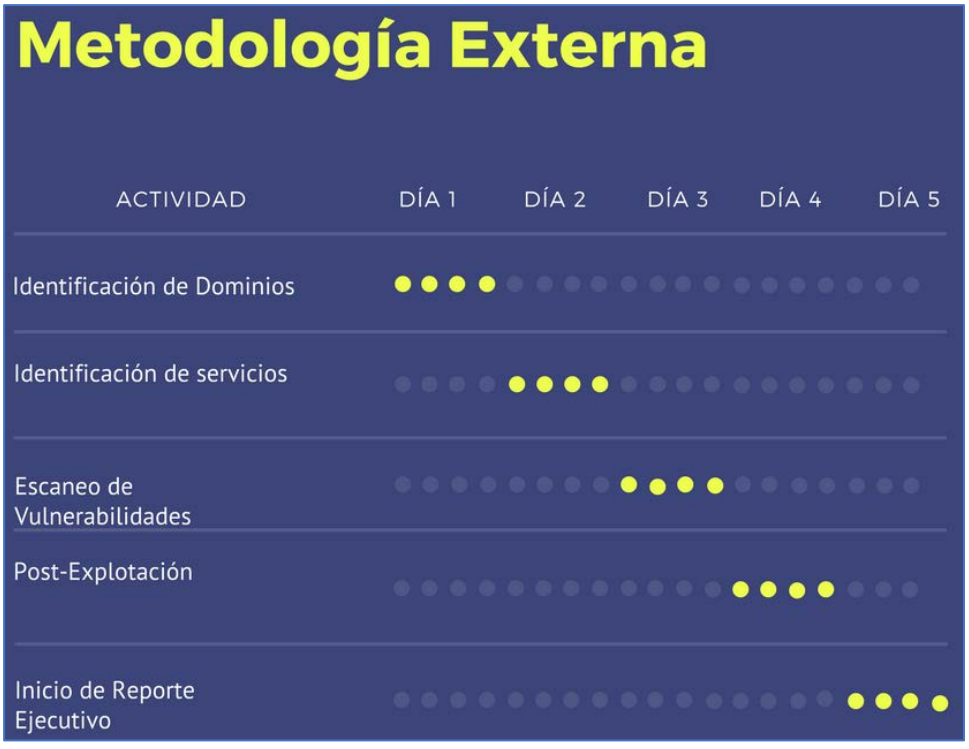


Ilustración 7. Metodología externa

1. **Identificación de dominios**

Etapa de reconocimiento de los registros de dominio relacionados a los clientes a los que se les realizaron las pruebas de penetración.

2. **Identificación de servicios**

A través de la identificación de dominios, podríamos encontrar servicios de correo electrónico, servicios proporcionados por terceros (Windows, Amazon, Google, entre otros).

3. **Escaneo de vulnerabilidades**

Se pone en marcha las herramientas institucionales, internas con la finalidad de obtener un nivel de madurez en la seguridad de la infraestructura de los activos alcanzables desde el internet.

4. **Post-explotación**

En este proceso se realiza la recolección de evidencias sobre vulnerabilidades que han sido explotadas.

5. **Inicio de reporte ejecutivo**

Se inicia la construcción del reporte que se entregará previo al inicio de las pruebas internas en donde contendrá la metodología utilizada, vulnerabilidades encontradas y explotadas, evidencias y recomendaciones.

III.2 Pruebas de penetración Interna

Es la evaluación interna del perfil de seguridad de la empresa consultora de seguridad informática desde la perspectiva de un empleado o de alguien que tiene acceso a los sistemas o de un hacker que ha obtenido acceso a la red de la empresa. Las pruebas de penetración internas nos permiten reducir el riesgo de un ataque por parte de empleados internos e implementar una arquitectura de seguridad en las redes informáticas. Una evaluación interna debe cubrir todos los nuevos tipos de ataques internos y no sólo probar los ataques convencionales. La metodología interna que he usado durante mi estancia en la consultora en seguridad informática se puede observar a continuación: (véase Ilustración 8)

Ilustración 8. Metodología Interna

1) **Escaneo de red**

Se realiza el escaneo de toda la infraestructura tecnológica de la empresa que se audita, accediendo a todos los puntos de la red para generar un mapeo de los dispositivos existentes.

2) **Escaneo de puertos y enumeración**

Una vez mapeados los dispositivos existentes, se hace un escaneo de los puertos que se encuentran abiertos y generando las validaciones correspondientes para generar comunicación con cada uno de ellos además de un ordenamiento y numeración por tipo de servicio.

3) **Detección de servicios**

En esta etapa se realiza la correlación entre el número de puerto encontrado en la fase de **escaneo de puertos y enumeración** con los servicios que se proveen en cada uno de ellos para así conocer proveedor y tipo de conexión que se realiza cada uno.

4) **Detección de vulnerabilidades**

Se realiza un escaneo de vulnerabilidades de manera manual y con apoyo de herramientas como **Nessus** para un obtener un panorama genérico del nivel de madurez en la seguridad informática de cada cliente que se analizó.

5) **Explotación**

Etapa de la metodología interna en donde se materializan los ataques a las vulnerabilidades encontradas durante la fase de "**detección de vulnerabilidades**" con excepción de las vulnerabilidades asociadas a una denegación de servicio.

6) **Post-explotación**

Etapa en donde se realiza la escalación en los privilegios en el sistema, equipo o servicio que ha sido vulnerado.

7) **Creación de persistencia**

En esta etapa se crean usuarios, grupos, procesos o cambios de permisos para la obtención de control de los sistemas, servicios y/o equipos en cualquier momento posterior a la explotación de las vulnerabilidades encontradas.

8) **Obtención de evidencia relevante**

En esta etapa se realiza la recolección de evidencia de cada vulnerabilidad explotada mostrando sólo el resultado de la misma.

9) **Creación de presentación ejecutiva**

Etapa de la metodología interna en donde se realiza la creación de diapositivas que muestren el objetivo, alcance, resultados e impacto de las vulnerabilidades

10) **Inicio de reporte final**

Etapa de la metodología interna en donde se realiza la documentación de cada uno de los procesos antes mencionados con la esquematización de las vulnerabilidades encontradas, una breve recomendación y mostrando el resultado de la explotación para el respaldo de cada prueba realizada dentro de la infraestructura del cliente.

CAPÍTULO IV. HERRAMIENTAS UTILIZADAS

Capítulo IV. Herramientas utilizadas

Para determinar el conjunto de herramientas funcionales para las pruebas de penetración, se analizó cada herramienta según su funcionalidad y escenario específico de cada cliente para no afectar infraestructura o flujo de servicio para los clientes. Se deben incluir los objetivos específicos a ser probados, las técnicas de pruebas de penetración, la gama de tipos de vulnerabilidades, la facilidad de uso y las variables puedan respaldar el cumplimiento de objetivos en los análisis.

Para el cumplimiento de los objetivos específicos de cada cliente, se realizó una configuración en particular de cada una de las siguientes herramientas:

a) Wireshark

Wireshark es el analizador de protocolo de red más importante y ampliamente utilizado en el mundo. Esta herramienta la usé para visualizar el tráfico que pasa a través de una red (cableada e inalámbrica), haciendo configuraciones para obtener información sobre qué protocolo pertenece y las opciones de reensamblado. Incluso si están cifrados, ayudando a la revisión del cumplimiento de controles de seguridad de las empresas clientes de la consultora en seguridad informática en donde laboré.

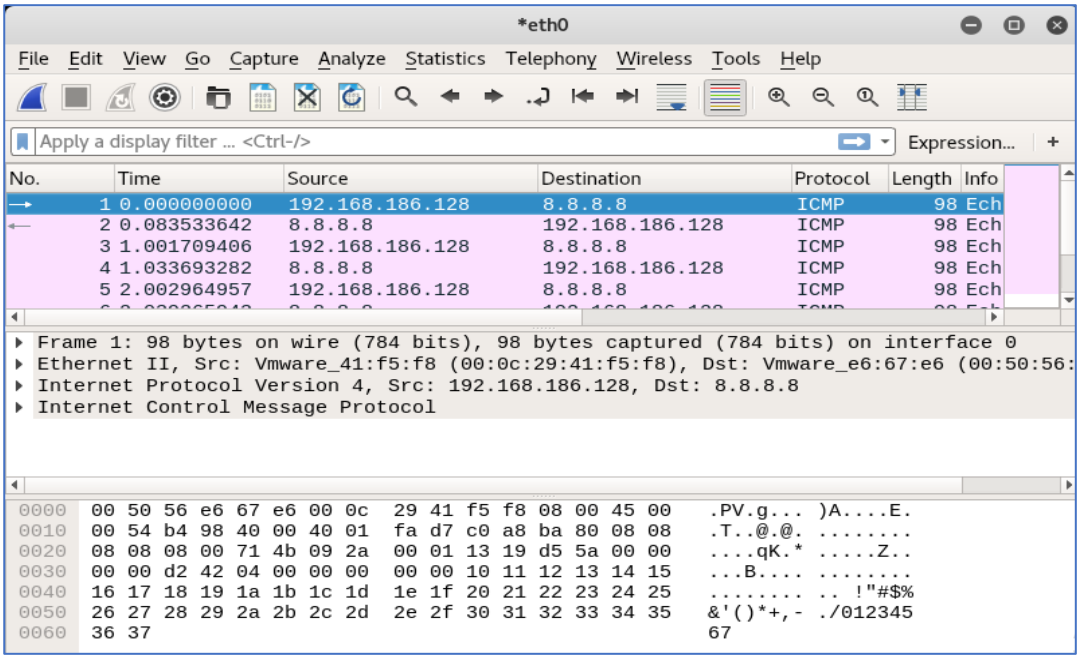


Ilustración 9. Uso de Wireshark

b) Angry IP scanner

Es un escáner, capaz de obtener direcciones IP en cualquier rango, así como en cualquiera de sus puertos. Sólo hace ping a cada dirección IP para verificar si está activa, y luego opcionalmente resuelve su nombre de host, determina la **dirección MAC**, escanea puertos, etc. El uso fue dado en redes que permitían realizar un escaneo sin protección o con permisos adicionados por dispositivos de red como firewalls o IDS's.

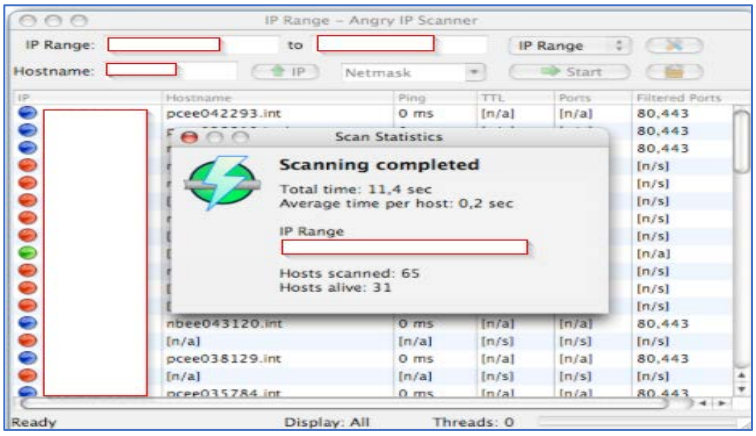


Ilustración 10. Uso de Angry IP Scanner

c) Nmap

Nmap ("Network Mapper") es una utilidad de código abierto y gratuito (licencia) para detección de redes y auditoría de seguridad.

Útil para tareas tales como inventario de red, administración de programaciones de actualización de servicio y monitoreo de tiempo de actividad de host o servicio.

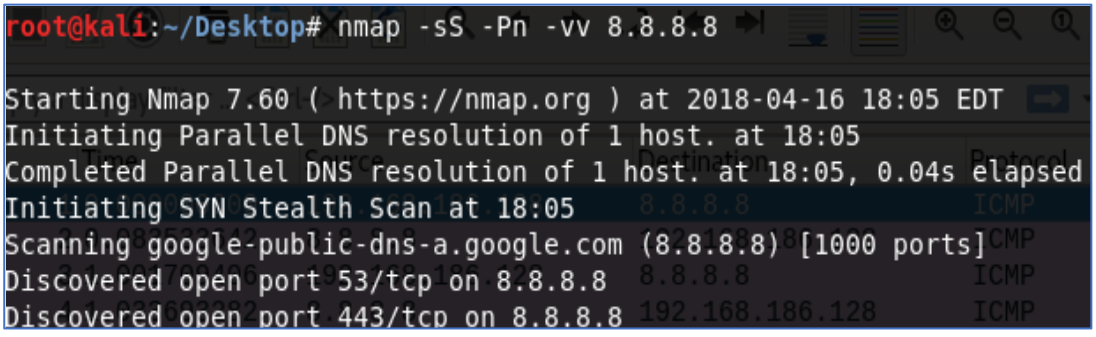


Ilustración 11. Uso de Nmap

d) Kali Linux

Es una distribución de GNU/Linux derivado de Debian, con soporte del equipo de offensive security que cuenta con una gama de más de 600 herramientas que vienen pre-instaladas para realizar pruebas de seguridad, las cuáles pueden ser escáneres de análisis de vulnerabilidades, reconocimiento de dispositivos en red, frameworks para la creación de exploits, robo de sesiones, cifrado y descifrado de datos, auditoría de bases de datos y muchas más que ocupé para las pruebas en diversas plataformas como sistemas operativos, plataformas móviles, portales web, etc.

Ilustración 12. Interfaz de Kali Linux

e) Nessus

Herramienta de evaluación más implementada de la industria para identificar las vulnerabilidades, problemas de configuración y malware que utilizan los atacantes para penetrar su red o la de su cliente con una interfaz fácil de usar.

Utilicé Nessus para la primera fase de escaneo de vulnerabilidades a nivel de aplicativos web y sistema operativo, obteniendo un primer estatus de la seguridad dentro de la institución, dando pauta a investigaciones sobre las vulnerabilidades encontradas, fases de autenticación en Windows y servicios como **SSH** y **TELNET**, además de la creación de certificados de confianza entre dispositivos.

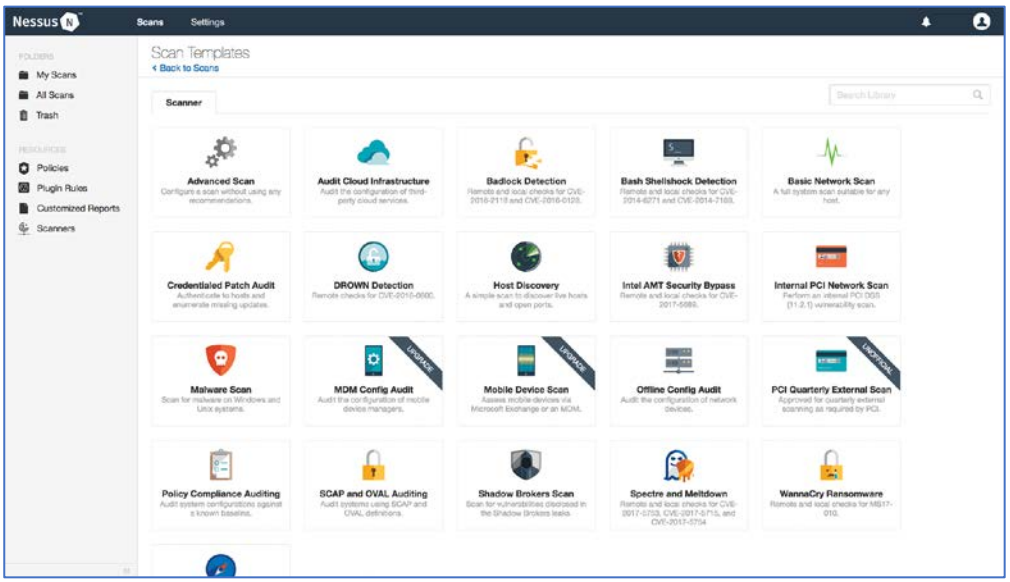


Ilustración 13. Uso de Nessus

f) VMWare

Es el software que apoya a la ejecución de múltiples sistemas operativos como máquinas virtuales en una única PC con Windows o Linux.

Herramienta utilizada en la creación de máquinas virtuales para realizar pruebas de penetración, simulación de sistemas operativos para retroalimentación para el departamento de seguridad ofensiva y simulación sistemas operativos para el escaneo de vulnerabilidades.

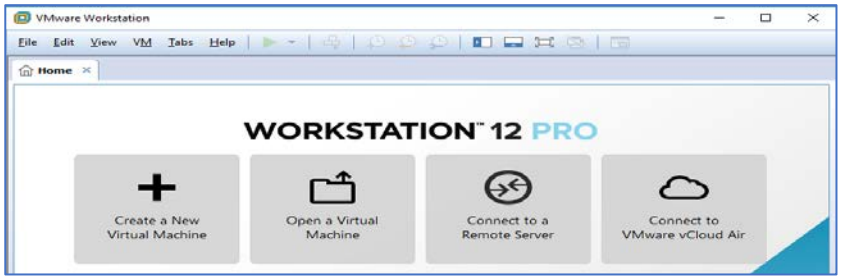


Ilustración 14. Uso de Vmware

g) Hyper-V

El rol del servidor de Hyper-V en Windows Server 2016 le permite crear un entorno informático de servidor virtualizado donde puede crear y administrar máquinas virtuales. Puede ejecutar múltiples sistemas operativos en una computadora física y aislar los sistemas operativos entre sí. Con esta tecnología, puede mejorar la

eficiencia de sus recursos informáticos y liberar sus recursos de hardware. Para las versiones más actuales de los temas en esta sección.

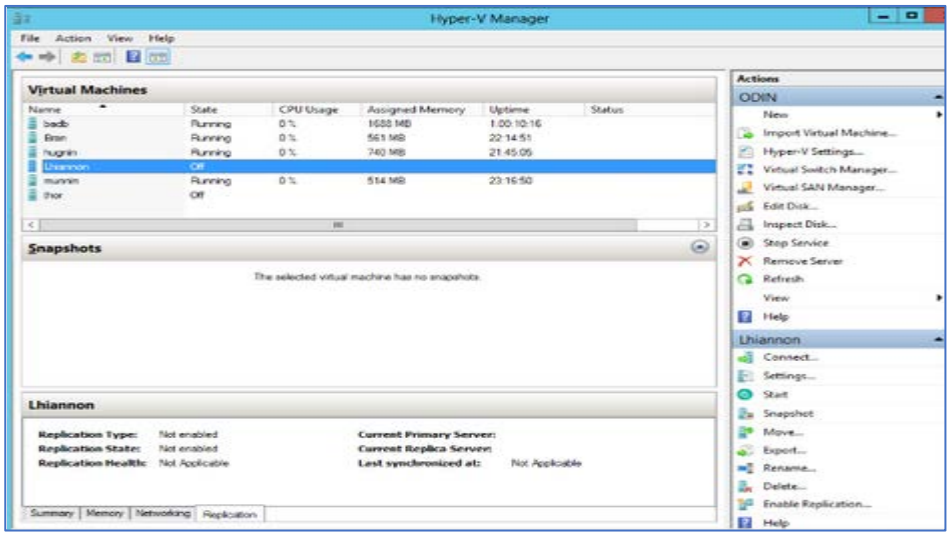
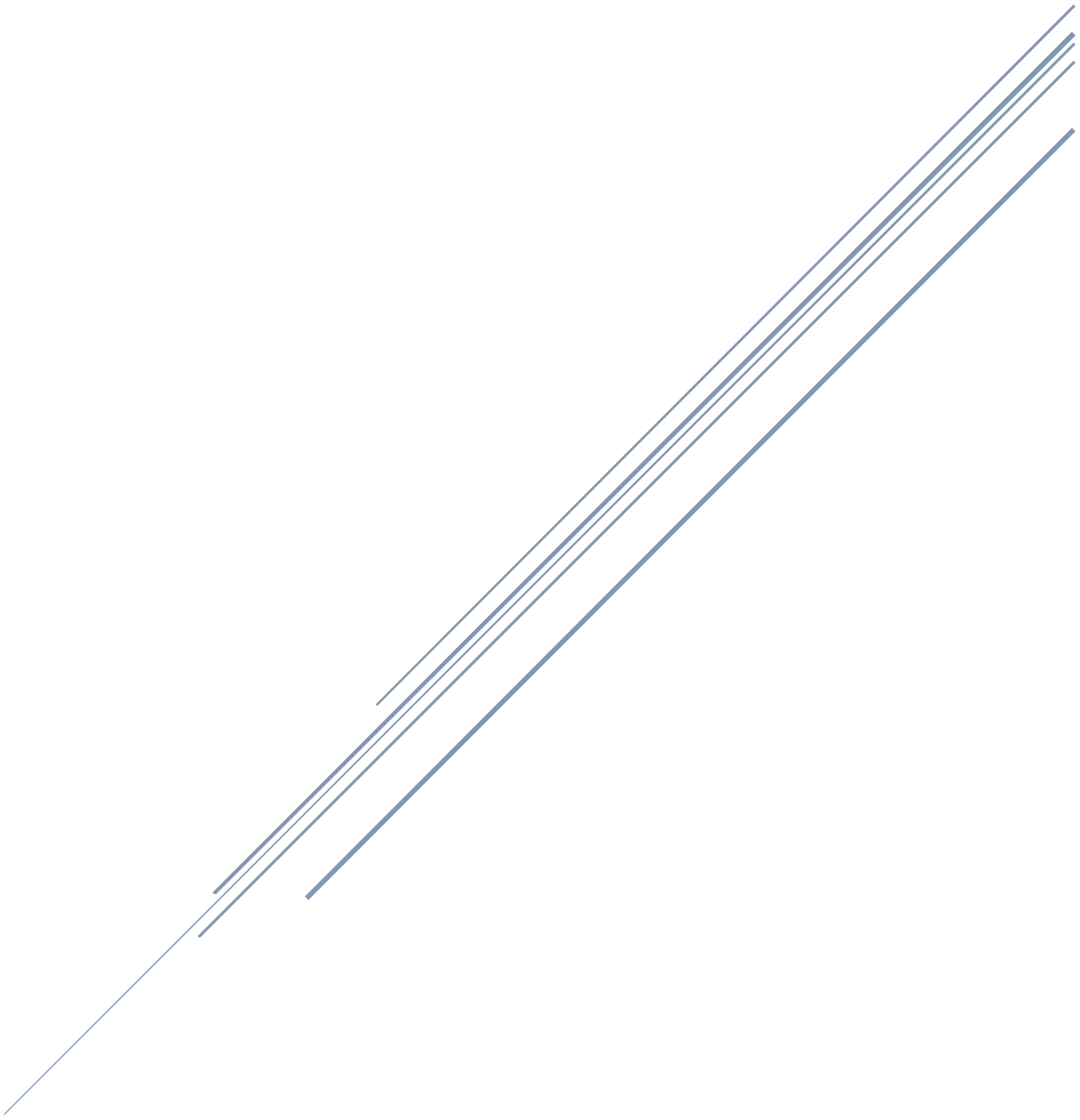


Ilustración 15. Uso de Hyper-V

CAPÍTULO V. ACTIVIDADES



Capítulo V. Actividades

Desde agosto de 2017 a mayo de 2018 laboré para una empresa consultora en seguridad informática cuyo nombre no puede ser revelado por los acuerdos de privacidad y confidencialidad que se firmaron por ambas partes. En esta consultora, realicé, apoyé y documenté diversos proyectos que tienen un enfoque de escaneo y explotación de vulnerabilidades de instituciones dedicadas a dos rubros: sector gobierno y sector financiero.

He realizado la instalación de diversas herramientas para la realización de escaneos e información básica de activos conectados a una red local, así como su configuración en la que, en cada proyecto se muestra una manera distinta de uso debido a limitaciones físicas o lógicas, simulando a un atacante que se encuentre en un entorno externo a la red local de la institución que se audite, así como de un atacante que ha ingresado a la red local y tiene conexión con cualquier activo que se encuentre dentro de la infraestructura organizacional.

El proceso de un análisis externo se lleva a cabo desde las oficinas de la empresa consultora en seguridad informática en donde he laborado, en las cuales se tiene la necesidad de evitar una denegación de servicio (DoS), una explotación de alguna vulnerabilidad que pueda afectar la disponibilidad del servicio que proporciona el cliente o impactar de manera directa a la operación del negocio.

El proceso de un análisis interno se lleva a cabo en las instalaciones del organismo que se audita, teniendo el acceso a un punto de la red interna de la organización, en donde el objetivo es recabar la cantidad mayor de información que pueda obtenerse, realizando un escaneo de puertos en los activos de la organización como lo son equipos de cómputo, routers, switch, access points, etc. En una etapa posterior al escaneo de puertos, se listan las vulnerabilidades, que se obtienen por medio de una exploración manual por parte del consultor o de herramientas propias de la consultora en seguridad, así como de software de terceros que son validados por el departamento de operaciones.

Con la información que obtenemos de los pasos anteriores, definimos los vectores de ataque posibles para realizar los intentos de explotación de las vulnerabilidades que cada activo posee, teniendo una diversidad que comprende un entorno web, un entorno de red local, entorno de red externa, malas configuraciones, contraseñas predecibles o por defecto, así como una captura del tráfico de red en activos inalámbricos para su análisis posterior. A los pasos anteriormente mencionados, se le conoce como etapa de ***post-explotación.***

Posterior a la etapa de explotación, se realiza la presentación ejecutiva para conocer junto con el(los) administrador(es) de los activos que presentaron una vulnerabilidad crítica y pudieron ser explotadas, analizando los controles evadidos y debilidades de configuraciones que fueron aprovechadas para la obtención de información sensible o control de activos.

Después de llevar a cabo la retroalimentación con el cliente, se realiza la documentación ejecutiva en donde se enlistará toda la evidencia y se realizarán recomendaciones generales para la mitigación de la vulnerabilidad, la cual será entregada al cliente después de un proceso de validación por el departamento de contraloría interna tanto de la empresa consultora en seguridad informática como de la entidad que ha sido analizada.

V.1 Participación profesional

En el departamento de seguridad ofensiva, participé como consultor de seguridad ofensiva en diversos proyectos, en los cuales realicé diversas actividades, desde escaneos para descubrimiento de puertos, servicios y dispositivos, hasta la explotación de vulnerabilidades existentes en los activos de cada organización en donde tuve la oportunidad de realizar pruebas de penetración.

Colaboré en la realización de presentaciones ejecutivas que fueron presentadas con las personas involucradas con la participación del proyecto en donde se encontraba el equipo de seguridad ofensiva de la empresa consultora en seguridad informática y el cliente, en donde acudían desde el director general de la empresa, área o departamento hasta los administradores de equipos y servicios que son analizados. En dichas reuniones se llevó a cabo una validación de los hallazgos encontrados presentado pruebas en tiempo real y evidencia obtenida durante el proceso de escaneo de vulnerabilidad y/o explotación.

En otras actividades, participé en la realización de documentación ejecutiva de los análisis externos ya sea a partir de archivos que contenían el registro de los escaneos realizados por algún miembro del equipo del departamento de seguridad ofensiva o por medio de los resultados obtenidos por la ejecución de mis herramientas y escaneos manuales.

Colaboré con cursos de seguridad informática que se impartieron en el departamento de seguridad ofensiva para cumplir con el objetivo con concientizar a los colaboradores de la empresa consultora en seguridad informática y a los clientes de la misma sobre la importancia de mantener un manejo adecuado sobre los activos que procesan información, así como manejo adecuado y seguro de herramientas y recursos brindados por el equipo seguridad informática al que pertenecí, disminuyendo así el riesgo para la información sensible de los colaboradores.

Apoyé a la realización de actividades de otros departamentos como lo es el área del centro de operaciones de seguridad, SOC por sus siglas en inglés (Security Operations Center), donde de requieren de la validación de existencia de vulnerabilidades, escaneo, determinación de falsos positivos y validación de criticidad de vulnerabilidades.

Apoyé a la creación de material para la capacitación del departamento de seguridad informática, en los rubros de sistemas operativos de Windows y GNU/Linux para la realización pruebas y brindar conocimiento sobre los vectores de ataque que se utilizan en las vulnerabilidades más conocidas y/o recientes en todo el mundo.

Participé en procesos que se lleva a cabo por el departamento de procesos para el cumplimiento de controles y requerimientos que se requieren en la obtención de certificaciones operativas para la empresa consultora en seguridad informática, realizando una auditoría interna en los activos que pertenecen a la infraestructura, así como a los equipos pertenecientes a los colaboradores de todas las áreas internas.

V.2 Proyecto entidad bancaria extranjera

V.2.1 Objetivo

Este proyecto se llevó a cabo en una entidad extranjera en donde el idioma inglés era predominante por lo que el objetivo primario era establecer una comunicación correcta entre el equipo de administración de seguridad de la empresa y los directivos de esta para poder así tener en claro sus necesidades y transmitirlas al equipo de seguridad ofensiva al que pertenecía. El objetivo principal podría visualizarse después de dicha fase de comunicación y era el poder obtener toda la información posible que se pudiera, sin ayuda por parte de la entidad bancaria, lo que significaba un análisis de caja negra.

El objetivo principal tenía varias fases en él, entre ellas era obtener la configuración correcta de las herramientas como máquinas virtuales, escáneres de puertos y servicios, escáneres de vulnerabilidades y cualquier otra que fuese a ser utilizada, por lo que se tenía que conocer la infraestructura que tenían, tipo de tecnologías, flujos de red y controles de seguridad que existieran en la entidad.

Además de los objetivos anteriores, se tenía un objetivo opcional, el cual consistía en la realización de una prueba de phishing sólo y sólo si, en las fases anteriores se lograran con éxito.

V.2.2 Descripción

En la metodología PTES se tiene la primera fase a cuál es el contacto previo o **Pre-requisitos** con el cliente, con el cual se conoció al administrador de seguridad de la entidad con quien se llevó a cabo una serie de acercamientos técnicos para conocer las condiciones en las que se encontraba la entidad bancaria en términos de controles de acceso, para saber cómo y desde dónde se podían comenzar a realizar las pruebas de penetración en la empresa así como las herramientas que podrían ser de utilidad o fueran de la preferencia del cliente para las pruebas requeridas y que no afectara la operación de sus sistemas, esto podría llevarse a cabo por el Project Manager y el equipo del departamento de seguridad al que pertenecí; esto se llevó a cabo en un sitio apartado de la infraestructura tecnologíca en sola visita a la entidad bancaria.

Posteriormente, en la fase **“recopilación de información”**, se obtuvo información precisa sobre los portales web, estructura de la empresa, tipo de sistemas operativos, activos de interés para el corporativo como lo son los servidores en

donde se llevaban a cabo algunas transacciones bancarias por medio del sistema de Pagos Electrónicos Interbancarios (SPEI), servidores de bases de datos de clientes y proveedores, entre otros, además de conocer los nombres de los empleados que dieron de alta el dominio de la entidad bancaria que estaba siendo auditada por el equipo de seguridad ofensiva, además de obtener correos y departamentos que la conformaban, que por razones de seguridad y privacidad no puedo describir en el presente documento ni mencionar las herramientas con las que lo llevé a cabo.

Así, pude dar comienzo con la fase de **modelado de amenazas**, en donde se debía realizar la siguiente pregunta: ¿Qué herramientas podría necesitar?, algo que me permitió realizar un análisis y configuración de herramientas como Nessus Professional y una máquina virtual de Kali Linux que me permitiera obtener la conectividad con todos los equipos dentro de la red de la empresa auditada, además de dispositivos físicos que me permitiesen obtener conectividad con todos los dispositivos de red.

Recordando que la fase de “modelado de amenazas” se basaba en mi juicio y preparación según experiencias previas, pues esta fase se llevaba a cabo en la consultora en seguridad en donde laboré.

En la fase de **análisis de vulnerabilidades** de la metodología PTES, realicé un análisis de vulnerabilidades por medio de las herramientas Nessus y Kali Linux, pruebas por medio de la ayuda de la suite de herramientas de Metasploit entre otras que darían una visión preliminar de la institución en donde se tenía que analizar cada salida y realizar un análisis profundo para la determinación de falsos positivos en donde realicé la investigación correspondiente así como las pruebas necesarias para filtrar toda la información obtenida y enfocar el esfuerzo en vulnerabilidades confirmadas y más críticas que dieran valor al escaneo y análisis que realicé, preparando la entrada para la fase de explotación.

Esta fase es la más conocida de la seguridad informática, en donde casi siempre se ven a individuos detrás de un ordenador con un aspecto misterioso y con tintes de maldad, pero en realidad, siendo un ethical hacker tuve que obtener información precisa para responder a la pregunta ¿Cómo es la seguridad de la infraestructura de la entidad bancaria?, siendo necesario el llegar a todos los puntos de la entidad bancaria.

En esta fase de la metodología suelen presentarse diversas complicaciones técnicas que dependen totalmente de la infraestructura del cliente que será

auditado, en esta entidad bancaria, se presentó un problema debido a un control de seguridad que se poseía en la comunicación a nivel red: **port security**. El port security servía para delimitar los equipos que pudiesen conectarse entre sí, por ejemplo, un ejecutivo de ventas que debía tener acceso a los portales web en donde se encontraba la información de alta para nuevo cliente, así como restringir el acceso para los servidores web ya que sólo deberían estar dispuestos para servidores y algunas transacciones provenientes de equipos específicos, por lo que surgió la necesidad de realizar una solicitud a los administradores de la red para que permitieran el paso de los dispositivos que destinó el equipo de seguridad ofensiva al que pertenecí, facilitando la visión estructural de la institución, por lo que se tuvo que enfocar el esfuerzo primario a conocer dicho flujo de información desde nuestro punto de análisis por medio de la herramienta Kali Linux y sus módulos de herramientas que posee. Así mismo, se tuvo conocimiento de los sistemas operativos que poseían y se especuló sobre el tipo de manejadores de información (Bases de Datos, Active Directory, entre otros), dando la facilidad de la creación de una serie de pasos para confirmar y vulnerar a dicho tipo de activos.

Después de obtener toda la información necesaria, realizar el análisis de vulnerabilidades, preparación de herramientas y entornos de explotación, pude ingresar a la fase de **explotación,** esta es la fase en donde obtuve acceso a servidores de importancia para la institución, colaboré con información necesaria para el ingreso a servidores de bases de datos y **SPEI**, elevación de privilegios en dispositivos que poseían información sensible sobre contraseñas, direcciones de red y parámetros requeridos para el ingreso a servidores sensibles para la institución, siendo una de las fases que más disfruté durante el seguimiento de la metodología **PTES** y de las más conocidas y asociadas a la palabra “hacker”. Debido al aviso de privacidad, no puedo describir los pasos que llevé a cabo, reservando más información en una presentación en donde se hable más a detalle sobre el presente escrito.

En la fase de **Post-Explotación** realicé el análisis del impacto que provocaría un ataque cibernético real, poniendo atención en el número de usuarios que ocupan la tecnología vulnerada, la criticidad de cada activo y el impacto a la operación de la entidad que generaría el tener inoperante algún servicio.

Esta fase la realicé teniendo contacto directo y presencial de la dirección de tecnologías de la entidad bancaria para poder determinar la importancia de cada activo y/o servicio y la criticidad que cada servicio poseía de manera interna, así como mostrar la posibilidad de parte del equipo de seguridad ofensiva al que pertenecía, para obtener acceso y/o posesión total o parcial de los servicios para

determinar la complejidad de llevarlo a cabo. En esta etapa pude saber que las bases de datos, el Active Directory y el servidor SPEI poseían un nivel de criticidad alta y, por lo tanto, tuve que detallar minuciosamente cada falla que se encontraba en los equipos y servicios dentro de los componentes antes mencionados.

Al finalizar la fase de **post-explotación**, se realizó la valoración de mi trabajo y la del equipo de seguridad ofensiva de la empresa consultora en seguridad en la que laboré, teniendo vía contrato una opción, en donde en caso de obtener acceso a vulnerabilidades de gran importancia e impacto para la entidad bancaria, así como comprobar la capacidad de llevarla a cabo sin mayor riesgo a impactar la operación de la entidad bancaria; habría una expansión de las actividades en las cuales se estableció realizar pruebas de phishing.

Así, comencé con la realización de un conjunto de técnicas de recolección de información de servidores de correo, así como conocer la estructura general, logos, departamentos y demás información asociada a los trabajadores de la empresa para poder replicarlo en un correo que fungiera como plantilla y pasara por oficial dentro de la institución, haciéndolo llegar a la directora de operaciones de la institución en México, dando un resultado positivo para el equipo ya que se logró de manera exitosa, cumpliendo el objetivo de obtener información sensitiva para la empresa.

En la fase de **reporteo**, colaboré con la preparación de la documentación de los hallazgos de seguridad obtenidos, en un formato conveniente para el entendimiento de un administrador o persona técnica y un reporte en donde se mostrara el riesgo y posibles problemas generados por la no continuidad del negocio debido a un posible ataque y explotación de las vulnerabilidades existentes en la institución bancaria, abriendo la puerta a la realización de una presentación de tipo ejecutiva mostrando los hallazgos más críticos y el impacto de su explotación en donde tuve la oportunidad de colaborar en su realización y explicación con directivos de la entidad bancaria provenientes del otro lado del mundo.

V.2.3 Alcance

Se requirió un enfoque de caja negra para este análisis sin realizar una explotación de vulnerabilidades que provocaran un impacto a la continuidad al negocio, teniendo el universo de todos los componentes de la institución de dentro de México para poder así obtener un estatus de sus activos de manera pertinente.

V.2.4 Contexto de la participación laboral

V.2.4.1 Descripción del problema

El problema principal al que me enfrenté, fue la existencia del **port security**; para realizar el reconocimiento de activos y obtención de Información que se describe en las primeras fases de la metodología se requiere la comunicación con los objetivos de la institución hacia todos los puertos abiertos que pudiera poseer por lo que la presencia del port security fué una delimitante para completar las fases mencionadas y dar pauta a los siguientes pasos de la metodología PTES por lo que se requirió la autorización de los administradores para llevar a cabo la conexión con la infraestructura, generando la necesidad de llevar a cabo la investigación para llevar a cabo la correcta configuración de las herramientas como máquinas virtuales y escáneres de vulnerabilidades para llevar a cabo las pruebas necesarias.

El problema más fuerte que se tenía en toda la infraestructura de la entidad bancaria era la falta de instalación de parches de seguridad en un gran número de servidores y equipos personales por lo que podría desembocar en ataques y comprometer la información sensible que posee cada dispositivo ya que eran susceptible a ataques de ransomware (**WannaCry),** elevación de privilegios entre otros.

El idioma fue una complicación debido a la gran cantidad de tecnicismos requeridos para la comunicación correcta en determinados momentos como lo fue la presentación ejecutiva y la creación del reporte ejecutivo en el idioma inglés.

V.2.4.2 Solución propuesta al problema

La solución de las problemáticas fueron las siguientes:

a. Port Security

Obtuve las **direcciones MAC** del adaptador de red y de las máquinas virtuales, así como realicé la configuración de máscaras de red, puertas de enlace y direcciones IP, así como la correcta configuración de Nessus, Kali Linux, escáneres de puertos y servicios, así como de las herramientas de auditoría de seguridad que se utilizan en las pruebas.

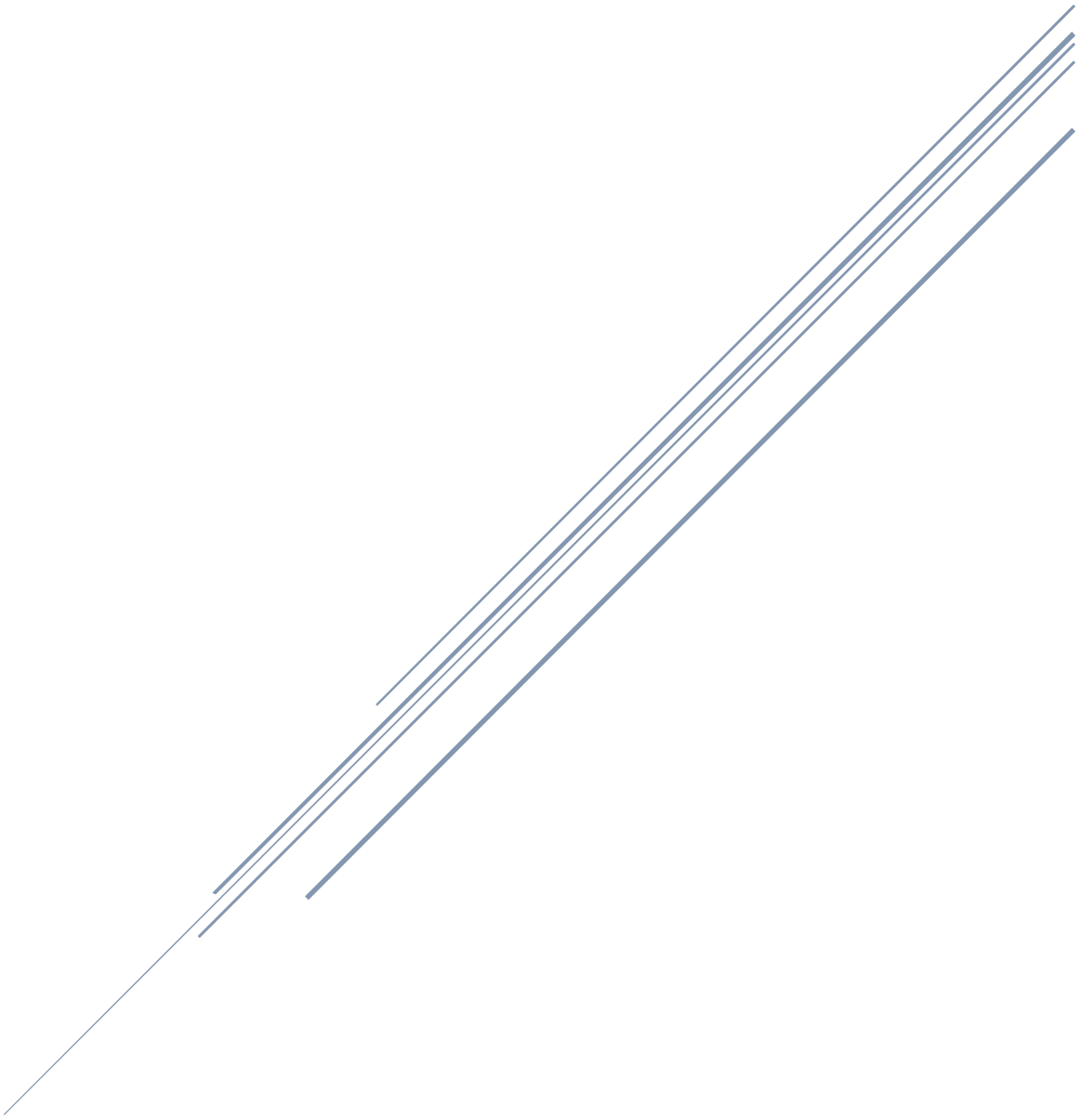
b. Idioma

Pude mantener conversación en el idioma inglés para comunicarme correctamente con los directivos de la empresa en la presentación ejecutiva investigando cada término de importancia y practicando la pronunciación de algunos tecnicismos del área de seguridad.

c. Parches de Seguridad

La investigación de cada vulnerabilidad fue una gran solución para conocer a fondo el alcance de la explotación en caso de que un cibercriminal llegara a tener la oportunidad de llevarla a cabo, dándome así la facilidad de conocer la manera de mitigar dicha vulnerabilidad y proveer una solución concisa a los administradores de los activos. La misma investigación, proporcionó la ayuda necesaria para la determinación de los falsos positivos que se encontraban derivados de dispositivos de seguridad y filtrado de paquetes que existían en la infraestructura de la entidad bancaria.

CAPÍTULO VI. RESULTADOS



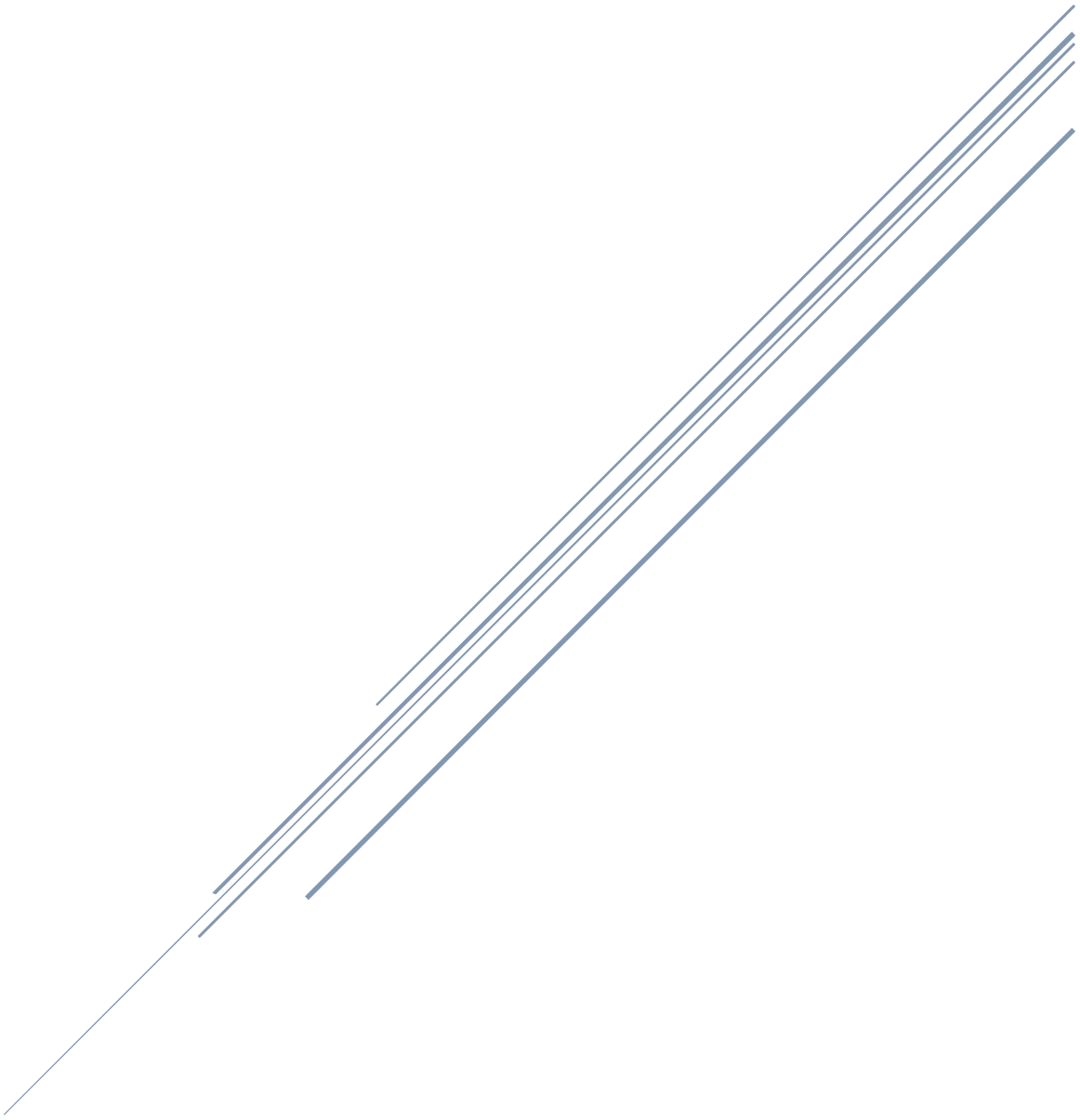
Capítulo VI. Resultados

Las fases de la metodología PTES ha sido compatible con la idea de negocio de la empresa consultora en seguridad informática en donde estuve laborando, dando un desglose benéfico de la información obtenida y generando un entregable para con el cliente, dando así un carácter más ordenado y provechoso en cuanto a vulnerabilidades encontradas y las soluciones para cada una de ellas.

Otro aspecto en el que pude obtener resultados ha sido el uso de herramientas, sabiendo la existencia de herramientas con licencia y herramientas de software libre; con el cliente, es importante presentarle herramientas que tienen soporte y un equipo respaldando el comportamiento de la herramienta, el renombre de la herramienta transmite tranquilidad y confianza, la curva de aprendizaje es adecuada para el cliente como para la empresa consultora en seguridad informática, evidenciando únicamente el ámbito monetario en donde una herramienta de esta índole, puede llegar a ser muy costosa. Pude darme cuenta de que no todas las herramientas que proporcionan valor a un servicio de pruebas de penetración, sino que herramientas de software libre también proporcionan información valiosa a las pruebas, generando una confianza al consultor o especialista de seguridad al realizar la comparación con herramientas que requieren licencia.

El ser un consultor de seguridad es una profesión que requiere amplio conocimiento en diferentes ramas de la tecnología, requiriendo formación constante y puntual, en donde el objetivo será ayudar a las empresas a mejorar en su seguridad interna y externa, proporcionando el mayor valor a su infraestructura, requiriendo sustentar una comunicación eficaz y directa para transmitir estas necesidades.

CAPÍTULO VII. CONCLUSIONES



Capítulo VII. Conclusiones

Gracias al avance tecnológico y a la creación de nuevas tecnologías de la información, el ámbito empresarial se ha beneficiado gracias al desarrollo de herramientas, sistemas y a la mejora en sus procesos, demarcando una gran documentación al respecto; cada avance conlleva una serie de riesgos y amenazas que crecen de la misma manera o inclusive de manera mayor para dichas tecnologías. En los últimos años, los ataques cibernéticos se han incrementado exponencialmente en el ámbito empresarial y de gobierno, surgiendo así la necesidad de la creación de áreas de seguridad informática, contratación de especialistas en incidencias cibernéticas en infraestructuras de tecnologías de la información; generando así una lucha interminable entre especialistas de la seguridad informática y los cibercriminales por la información de los grandes corporativos.

Al concluir mi participación en los proyectos de análisis de vulnerabilidades y pruebas de penetración en la empresa consultora en seguridad, pude identificar hallazgos de seguridad que serían los iniciadores de afectaciones en los pilares de la seguridad: confidencialidad, integridad y disponibilidad dentro de las instituciones en donde realicé dichas pruebas, así pude conocer que pérdidas económicas, pérdida de clientes, pérdida de confianza en la institución e impacto en la continuidad del negocio son ámbitos que pueden ser afectados por una incidencia de seguridad, por lo cual, las empresas cada vez invierten mayor cantidad de recursos en la seguridad informática.

Las empresas, también buscan evitar la inversión en esta área, tratando de implementar algún tipo de capa extra de seguridad sin la ayuda de especialistas del área, como lo son software/hardware que implementen tipos de filtrado en los paquetes de comunicación, exponiéndose así a otro tipo de ataques o peor aún, concentrando su seguridad en un solo dispositivo. También, la problemática más común pude encontrar que es la falta de parches de seguridad, en donde se hace uso de software obsoleto que da la facilidad de brindar el control total del dispositivo, así como la falta de soporte del proveedor en algunos casos y el mal diseño o seguimiento de malas prácticas por las áreas de desarrollo de software.

Por medio del rol que asumí durante los proyectos de análisis de vulnerabilidades y pruebas de penetración, colaboré con la realización de las pruebas, la investigación de las vulnerabilidades, corroboré el uso correcto de cada herramienta, así como los posibles errores que llegaran a surgir según cada entorno de las diversas instituciones en donde se llevaban a cabo las pruebas.

Para asegurar el éxito, pude corroborar que la metodología PTES es adecuada para obtener el resultado esperado por las instituciones, facilitando el aspecto técnico y obteniendo fallas de seguridad que pudieron ser aprovechadas por mí.

CAPÍTULO VIII. BIBLIOGRAFÍA

Bibliografía

Angryip.org. (2018). About. [Online] Recuperado del sitio:

http://angryip.org/about/

Arroyo, M. (2011). SE Hacking Ético: Google Hacking – Parte 1. [online] Hacking Ético. Recuperado del sitio:

https://hacking-etico.com/2011/07/20/se-hacking-eticogoogle-hacking-parte-1/

Banxico. (2019). ¿Qué es cómo funciona el SPEI? [Online] Recuperado del sitio:

https://www.banxico.org.mx/spei/d/%7B44351472-054C-58EB-611D-153B1029C2A8%7D.pdf

Certsuperior. (2018). Seguridad informática. [Online] Recuperado del sitio:

https://www.certsuperior.com/seguridadinformatica.aspx

Eset. (2018). ¿Qué es un 0-day? Explicando términos de seguridad. [Online] Recuperado del sitio:

https://www.welivesecurity.com/la-es/2015/02/25/que-es-un-0-day/

forodeseguridad.es. (2018). El consultor de seguridad ¿Qué significa ser consultor en Seguridad? [Online] Recuperado del sitio:

http://www.forodeseguridad.com/artic/reflex/ref_8036.htm

Icorp. (2018). Microsoft Hyper-V. [Oline] Recuperado del sitio:

http://www.icorp.com.mx/solucionesTI/MicrosoftHyperV/

Instituto Nacional de Tecnologías Educativas y de Formación del profesorado. (2018). Elementos vulnerables en el sistema informático. [Online] Recuperado del sitio:

http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/elementos_vulnerables_en_el_sistema_informtico.html

ISACA. (2018). La integridad de los datos: el aspecto más relegado de la seguridad de la información [Online] Recuperado del sitio:

https://www.isaca.org/Journal/archives/2011/Volume-6/Pages/Data-Integrity-Information-Securitys-Poor-Relation-spanish.aspx

Kaspersky Lab. (2018). Las vulnerabilidades de software. [Online] Recuperado de:

https://securelist.lat/threats/las-vulnerabilidades-de-software/

Marvin G. Soto. (10 de enero, 2016). (Penetration Test y Seguridad con Herramientas Libres. [Online] Recuperado del sitio: *https://medium.com/@marvin.soto/penetration-test-y-seguridad-con-herramientas-libres-2fa219b5bdb8)*

Mendoza, M. (2015). ¿Ciberseguridad o seguridad de la información? Aclarando la diferencia. [Online] WeLiveSecurity. Recuperado del sitio:

https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridadinformacion-diferencia/

Microsoft. (7 de octubre, 2016). Hyper-V on Windows Server 2016 [Online]. Recuperado del sitio:

https://docs.microsoft.com/es-mx/windows-server/virtualization/hyper-v/Hyper-V-on-Windows-Server

Neuvoo. (2017). ¿Qué hace un Consultor de Seguridad? [Online] Recuperado del sitio:

https://neuvoo.com.mx/neuvooPedia/es/consultor-de-seguridad/

Pentest-standard.org. (2014). Organización de alto nivel del estándar. [Online] Recuperado del sitio:

http://www.pentest-standard.org/index.php/Main_Page

Red Hat. (2018). Manual de seguridad. [Online] Recuperado del sitio:

http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/s1-sgs-ov-controls.html

Seguritecnia.es. (2018). Cambio de rol de la figura del consultor de seguridad [Online] Recuperado del sitio:

http://www.seguritecnia.es/seguridad-privada/seguridad-integral/cambio-de-rol-de-la-figura-del-consultor-de-seguridad

Symantec. (2018). Glosario de Seguridad. [Online] Recuperado del sitio:

https://www.symantec.com/es/mx/theme.jsp?themeid=glosario-de-seguridad

Universidad del Claustro de Sor Juana. (noviembre 2016). [Online] Ética hacker, seguridad y vigilancia. Recuperado del sitio:

http://elclaustro.edu.mx/pdf/EticaHackerSeguridadVigilancia.pdf

Wireshark.org (2018). About Wireshark. [Online] Recuperado del sitio:

https://www.wireshark.org/

CAPÍTULO IX. ANEXOS

Capítulo VIII. Anexos

A continuación, se muestran algunos fragmentos de actividades realizadas durante la realización de diversos trabajos para la empresa consultora en seguridad informática. En esta sección, se realizará un repaso de manuales, lo que ha permitido la instalación y explotación de vulnerabilidades en diferentes escenarios y en las instalaciones de clientes en las que se realizaron ciertas configuraciones para obtener un mejor resultado.

También, se crea un glosario para un mejor entendimiento del contenido que se ha descrito en este informe de actividades profesionales, esperando el esclarecimiento de cualquier duda acerca de términos técnicos y conceptuales que giran al entorno de la seguridad de la información.

VIII.1 Creación de Maquetas

Objetivo

Crear equipos virtuales con diversos sistemas operativos y versiones de estos para el análisis de sus componentes, generando la facilidad de crear nuevos vectores de ataque y abriendo la posibilidad de tener más versatilidad para con los clientes de consultora en seguridad donde laboré.

Descripción

La necesidad de un profesional de la ingeniería sobre conocer un poco más de manera constante para obtener los conocimientos más recientes y proveer las mejores soluciones a su sector, me ha brindado la habilidad de investigar sobre temas específicos y los que se me han requerido; adquiriendo conocimiento. Así, en esta sección describo la tarea que se me dio en realizar la virtualización de máquinas virtuales con el apoyo de la herramienta Hyper-V en un entorno nativo con Windows Server 2016 Standard Edition.

Antecedentes

Hyper-V es el producto de virtualización de hardware de Microsoft que permite crear y ejecutar una versión de software de una computadora, llamada máquina virtual. Cada máquina virtual actúa como una computadora completa, ejecutando un sistema operativo y programas, así mismo, cuando necesitan recursos informáticos las máquinas virtuales le brindan más flexibilidad, proporcionan apoyo para ahorrar tiempo y dinero, y son una forma más eficiente de usar hardware que simplemente ejecutar un sistema operativo en hardware físico. Hyper-V ejecuta cada máquina virtual en su propio espacio aislado, lo que significa que se puede ejecutar más de una máquina virtual en el mismo hardware al mismo tiempo. Esta técnica es de gran ayuda para evitar problemas como un bloqueo que afecte a las otras cargas de trabajo, o para dar acceso a diferentes personas, grupos o servicios a diferentes sistemas.

La utilidad, compatibilidad y su uso fácil que tiene Hyper-V, fue el motivo de su elección como software de virtualización. Compartí los temas necesarios con mi equipo de trabajo y se tomó la postura de abrir puertas a nuevas tecnologías que no se conocieran tanto, teniendo el conocimiento de que yo conocía la herramienta, su uso y potencial para la creación de máquinas virtuales. Así, a continuación, mostraré un fragmento de la documentación técnica realizada para el equipo de seguridad ofensiva de la empresa consultora en seguridad informática:

Para iniciar, en el servidor local (en este caso **192.168.1.120**[1])[1], dar click derecho y seleccionar la opción de “Nuevo”, seleccionar la opción “Máquina virtual…”

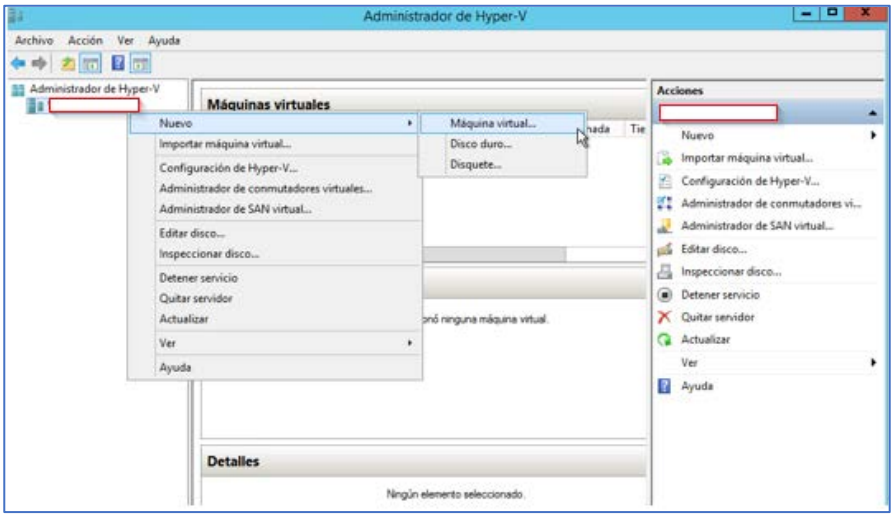


Ilustración 16. Creación de la nueva máquina virtual de Windows Server 2016

En una de las ventanas de instalación, se requiere hacer referencia sobre la ubicación de la imagen del sistema operativo a instalar, mostrando una imagen similar a la siguiente:

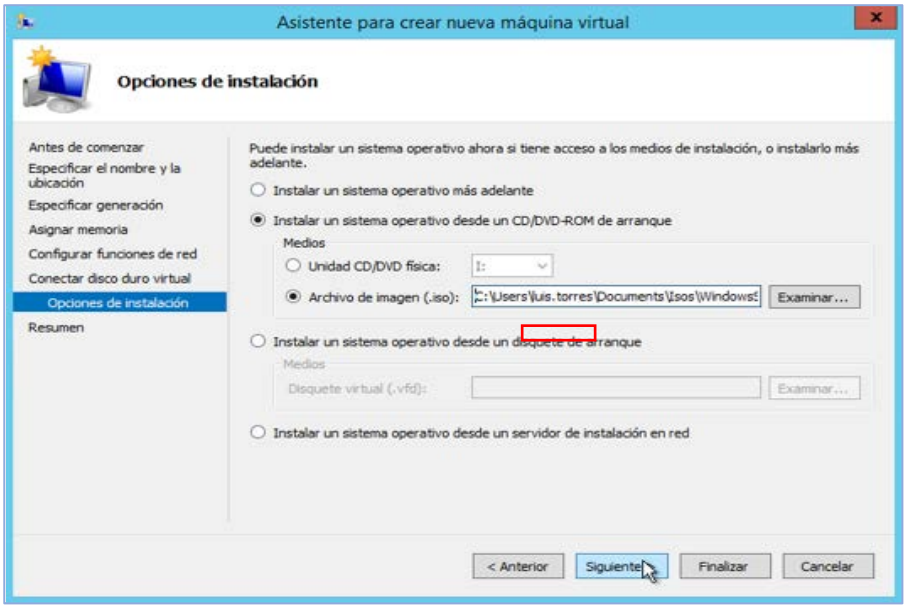


Ilustración 17. Selección del medio de instalación para Windows Server 2016

[1] Dirección IP cambiada por motivos de privacidad de la empresa consultora de seguridad informática

En la siguiente imagen se muestra el inicio de instalación del idioma del sistema operativo deseado:

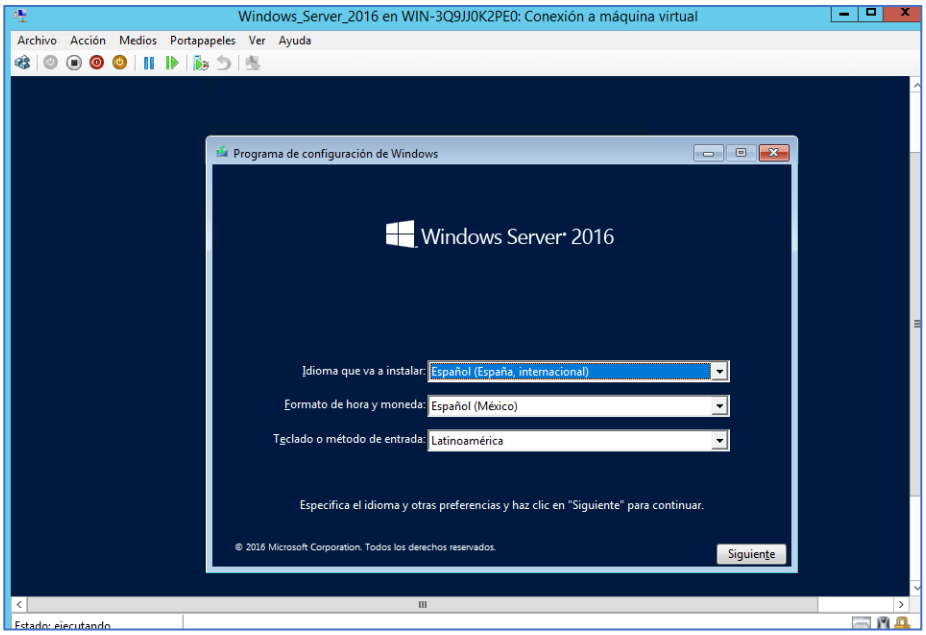


Ilustración 18. Selección de idioma en el sistema operativo

Posteriormente, se realiza la selección de la versión de la cual se hará la instalación, ya que es importante mencionar que cada versión puede poseer vulnerabilidades diversas que dependen del uso y finalidad para la que haya destinado su instalación.

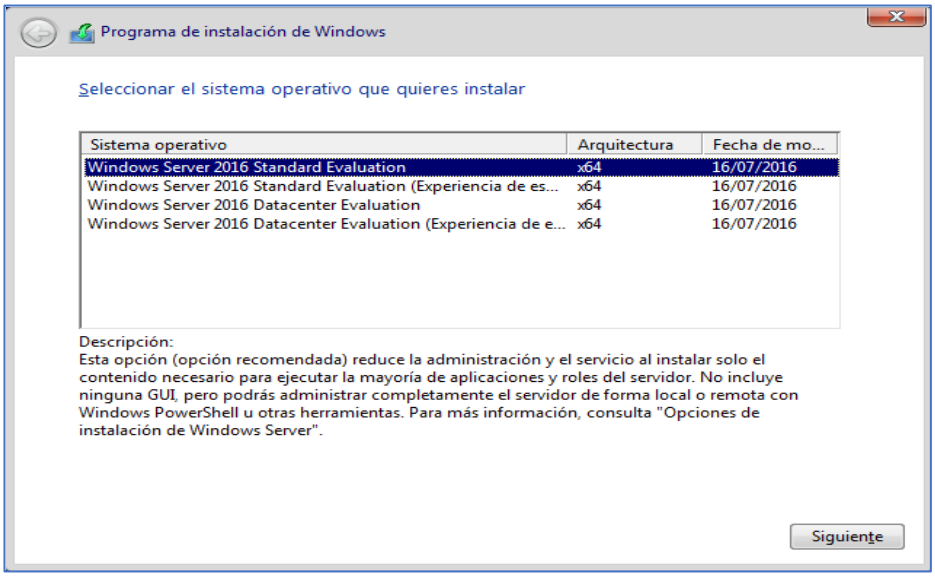


Ilustración 19. Selección de la versión de Windows Server 2016

Tras completar el proceso de instalación, se pudo observar el inicio del sistema operativo en la plataforma de Hyper-V.

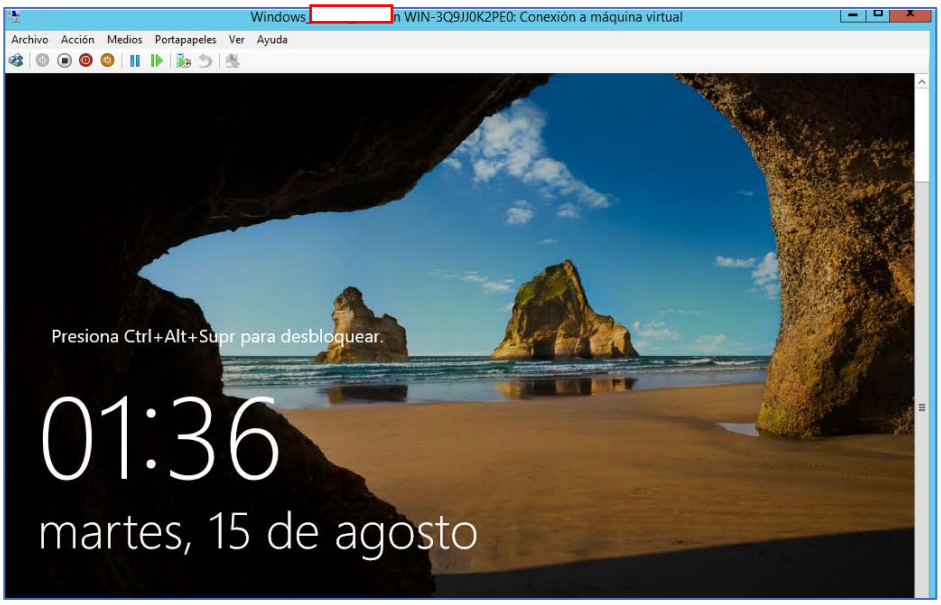


Ilustración 20. Visualización de la interfaz de bienvenida en Windows Server 2016

Nota: El sistema operativo Windows 2016 fue obtenido desde la página oficial de Microsoft https://www.microsoft.com/es-es/evalcenter/evaluate-windows-server-2016 por lo que cada una de las imágenes mostradas son producto de la instalación del sistema operativo antes mencionado.

VIII.2 Glosario

En esta sección, se describen algunos conceptos que fueron utilizados en todo el documento y que es preciso dar una descripción para proporcionar un mejor entendimiento en el manejo de cada uno.

Activo

Cualquier recurso que tiene valor, importancia y/o relevancia para la organización que lo posee.

Access point

Dispositivo de red que permite interconectar dos o más dispositivos para generar flujo de información entre ellos de manera inalámbrica.

Backend

Es la labor de ingeniería que compone el acceso a bases de datos y generación de plantillas del lado del servidor. Desarrollo en componentes del servidor con lenguajes de programación (PHP, Ruby on Rails, Django, Node.js, .NET).

DarkNet

Se refiere a una parte de la DeepWeb en la que se encuentra contenido ilegal como venta de armas, drogas, antigüedades, entre otras más.

DeepWeb

Se refiere a una red informática que almacena contenido no indexado en una red convencional y que ningún buscador convencional como Google o Bing acepta en sus reglas de servicios y por ello no lo provee.

Defacement

Es la modificación del contenido de un sitio web sin autorización del administrador para provocar un impacto en la imagen de una empresa y así obtener reputación para quien lo realiza.

Dirección MAC

Sus siglas en inglés significan Media Access Control y es el identificador único asignado por el fabricante a una pieza de hardware de red y cada código tiene la intención de ser único para un dispositivo en particular.

DoS

Es un ataque a un sistema de computadores o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

Escaneo de vulnerabilidades

Es la identificación, análisis y reporte sistemático de las vulnerabilidades de seguridad técnica que terceros e individuos no autorizados pueden usar para explotar y amenazar la confidencialidad, integridad y disponibilidad del negocio, los datos técnicos y la información.

Estándar de seguridad

Son acuerdos (normas) documentados que contienen especificaciones técnicas u otros criterios precisos para ser usados consistentemente como reglas, guías, o definiciones de características. para asegurar que los materiales productos, procesos y servicios se ajusten a su propósito.

IDS

Se refiere a un dispositivo o software que realiza una escucha del tráfico de red para analizarlo y así detectar actividades anormales y/o sospechosas, reduciendo el riesgo de una intrusión a un sistema.

Impacto

El impacto es la medición y valoración del daño que podría producir a la organización un incidente de seguridad dependiendo de la importancia que posea en recurso al que se produce este evento.

Incidencia informática

Estado de un proceso distinto a un comportamiento esperado, que puede tener alguna repercusión en la disponibilidad, integridad y a su confidencialidad.

JavaScript

Es un lenguaje de programación interpretado. Se define como orientado a objetos, basado en prototipos, imperativo, débilmente tipado y dinámico que se puede observar por medio de los navegadores web.

Licitación

Es un procedimiento, en virtud de que se compone de una serie de actos regulados por normas administrativas. Ese procedimiento tiene como finalidad seleccionar a la persona, física o jurídica, con la cual la administración pública habrá de celebrar un contrato determinado.

Port security

Es una función en los Cisco switch destinada a limitar la cantidad de direcciones MAC que se pueden conectar a través de un puerto.

Project Manager

Persona encargada de realizar el seguimiento de un proyecto, desde el inicio y determinación de alcance de este, realizando un seguimiento con el cliente y equipo de trabajo para el cumplimiento del proyecto satisfactoriamente.

Protocolo

Es un conjunto de reglas establecidas para permitir comunicar nodos de computadoras o equipos entre sí.

Ramsomware

Es un software malicioso que al infectar nuestro equipo le da al ciberdelincuente la capacidad de bloquear un dispositivo desde una ubicación remota y encriptar nuestros archivos quitándonos el control de toda la información y datos almacenados.

Riesgo

Es la posibilidad de que se produzca un impacto determinado en un activo, en un dominio (conjunto de activos) o en toda la organización; este impacto se puede producir debido a que una amenaza explote vulnerabilidades para causar pérdidas o daños.

Router

Es un dispositivo de red que realiza el trazado del flujo de información de un tráfico de datos, generando la ruta más apropiada y rápida para que lleguen a su destino.

Seguridad Perimetral

Se refiere a los controles y mecanismos de seguridad dentro y alrededor del centro de procesos de datos, así como los medios de acceso remoto al y desde el mismo, implementados para proteger el hardware y medios de almacenamiento de datos.

SPEI

Sistema de Pagos Electrónicos Interbancarios, es la infraestructura de pagos del Banco de México que permite a sus participantes, (bancos, casas de bolsa, socios y otras entidades financieras reguladas) enviar y recibir pagos entre sí para poder brindar a sus clientes finales el servicio de transferencias electrónicas en tiempo real.

SSH

Es un protocolo de administración remota que permite a usuarios controlar y modificar servidores remotos a través de una red utilizando técnicas criptográficas para garantizar que todas las comunicaciones hacia y desde el servidor remoto sucedan de manera cifrada.

Switch

Es un dispositivo de interconexión de equipos en una red, formando una red local, estableciendo sus especificaciones técnicas en el estándar conocido como Ethernet.

Telnet

Es un protocolo de red que permite acceder a otra máquina para el envio de comandos y así ejercer un manejo de manera remota.

Wannacry

Es un ransomware que tuvo un apogeo importante durante el mes de mayo de 2017 y atacaba a las redes aprovechándose de algunos protocolos de comunicación en sistemas Windows.