ISSN 2960-8236

Análisis de metodologías para pruebas de penetración y usabilidad para PYMEs

Diego Ortega-Garcés[1]
[1]Instituto Superior Tecnológico Quito
diego.ortega@itq.edu.ec
Corresponsal: diego.ortega@itq.edu.ec; Telf.: +593 962935297

Resumen: El propósito de este artículo es presentar las metodologías y estándares actuales utilizados por los profesionales de seguridad informática en las Pruebas de Penetración o Pentest. Se detallarán las fases, etapas y actividades involucradas en su ejecución. Estas pruebas son llevadas a cabo por especialistas que adoptan la perspectiva de un ciberdelincuente, con el objetivo de realizar ataques controlados a la infraestructura objetivo para identificar y mitigar posibles vulnerabilidades, así como frustrar ataques avanzados. La importancia de estas metodologías radica en su respaldo por organizaciones y comunidades especializadas de renombre, consideradas referentes en el campo de las pruebas de penetración. En la actualidad, esta actividad desempeña un papel fundamental en el ámbito de la seguridad, ya que proporciona información relevante sobre vulnerabilidades y amenazas que podrían comprometer la infraestructura tecnológica de cualquier organización.

Palabras claves: Amenaza, vulnerabilidad, seguridad, explotación, hacking ético, riesgo, pruebas de penetración, pentest y ataque.

Abstract: The purpose of this article is to present the current methodologies and standards used by computer security professionals in Penetration Testing or Pentesting. The phases, stages and activities involved in their execution will be detailed. These tests are carried out by specialists who adopt the perspective of a cybercriminal, with the objective of performing controlled attacks on the target infrastructure to identify and mitigate possible vulnerabilities, as well as to thwart advanced attacks. The importance of these methodologies lies in their endorsement by renowned organizations and specialized communities, considered benchmarks in the field of penetration testing. Today, this activity plays a fundamental role in the field of security, as it provides relevant information on vulnerabilities and threats that could compromise the technological infrastructure of any organization.

Keywords: Threat, vulnerability, security, exploitation, ethical hacking, risk, penetration testing, pentest and attack.

Artículo de revisión

Cita: Ortega-Garcés. Análisis de metodologías para pruebas de penetración y usabilidad para PYMEs. Revista DOXA, 1(1), 004 https://itq.edu.ec/wp-content/uploads/2023/06/2023-04-04_doxa_1-1-4-1.pdf

Recibido: 23/02/2023
Aceptado: 04/04/2023
Publicado: 23/06/2023

Santiago Del Castillo G., M.Sc.
Editor en jefe, Revista DOXA ITQ
Quito, Ecuador

1. Introducción

La información es un recurso vital para toda organización, ya que es considerada como uno de sus activos más importantes y el buen manejo de esta puede significar la diferencia entre el éxito o el fracaso. En este sentido, existe gran preocupación y esto ha motivado a que las empresas inviertan ingentes recursos para implementar y mejorar sus sistemas de seguridad (física, lógica y ambiental). En el mundo globalizado en el que las empresas se desempeñan es necesario estar interconectadas, es por eso que los sistemas de información se plantean como una respuesta para contar con un proceso permanente de recolección, procesamiento, presentación, interpretación, uso, y aplicación de la información en la toma de decisiones, redefinición de objetivos, recursos y estructuras de la organización. Es aquí donde, la ciberseguridad ha adquirido un valor relevante, ya que tiene que ver con la protección digital de activos; sin embargo, es imposible asegurar en su totalidad la información, ya que siempre existirán factores de riesgo (internos y/o externos) que se deben asumir, transferir o eliminar (Perrenoud, 1990)

Así como los avances tecnológicos permiten mayor acceso a las comunicaciones, estos plantean nuevos retos tanto para las empresas que adoptan medidas de seguridad ante las nuevas amenazas en el ciberespacio, como para los usuarios que deben adaptarse a las nuevas tecnologías, ya que en la actualidad la mayoría de actividades que las personas cotidianamente realizan, se manejan a través de las redes y por ende estas no cuentan con las debidas medidas de seguridad. En tal razón, los usuarios están cada vez más expuestos en la red, ya sea por desconocimiento o por negligencia en el cumplimiento de las políticas de cada organización, lo cual representa un riesgo.

La falta de conciencia referente a la seguridad de la información ha permitido que muchos ciberataques se hayan ejecutado con éxito. A pesar de no existir una definición clara, para efectos de este estudio se considerará un ciberataque como aquel que se aprovechan de las vulnerabilidades del software para tener acceso a él con el fin de destruir, alterar o interrumpir el sistema cibernético o físico asociado; sin embargo, junto con la definición y para poder conceptualizar y analizar los ciberataques, resulta necesario considerar una serie de elementos, entre estos: los actores involucrados, la ubicación, los medios, jurisdicciones y los motivos detrás de la realización de los mismos; así, podemos citar algunos de los ataques que comprometieron los datos de importantes organizaciones y estados(Recalde Caicedo, 2019)

Phillips (2019), la empresa que provee servicios a 300.000 clientes en todo el mundo, incluyendo el Ejército de EE.UU., el Pentágono, el Departamento de Estado, de Comercio, el de Tesoro y la Oficina presidencial estadounidense., entre otras entidades, reconoció que había sufrido un ataque virtual. Sus sistemas habían quedado comprometidas a causa de un código malicioso altamente sofisticado y extremadamente dirigido. Añadieron que el hecho se originó probablemente por parte de un Estado entre marzo y junio de este año, y que es posible que unos 18.000 de sus clientes resultaron afectados. El secretario de Estado de EE.UU., Mike Pompeo, culpó a Rusia de lo que se describe como el peor ataque de ciber espionaje contra el gobierno estadounidense. Cabe recordar que desde que se conoció el escándalo de Cambridge Analytica, la filtración de los datos de más de 87 millones de usuarios (136.985 españoles), Facebook se encuentra en el ojo del huracán. Investigada en Estados Unidos, la plataforma fue condenada en julio a pagar una multa de 5.000 millones de dólares por su gestión de la privacidad de los usuarios. A su vez, está siendo controlada de cerca por la FTC (Comisión Federal de Comercio) estadounidense (Cubillo Arribas, 2014).

Con estas cifras alarmantes y los constantes avances tecnológicos, es evidente que la tendencia de las empresas es la transformación digital, lo que implica mayores

riesgos sobre los activos de información que se quiere proteger, sin embargo, es preciso que las organizaciones estén actualizándose permanentemente, a fin de mantenerse vigentes y acordes a los avances tecnológicos.

Si bien es cierto estos avances brindan mayores facilidades, se debe tomar en cuenta también que los ciberdelincuentes estarán a la expectativa del más mínimo error y aprovechar para explotar las vulnerabilidades que consciente o inconscientemente por desconocimiento y/o negligencia, están presentes en toda infraestructura tecnológica. Por lo tanto, es preciso que las organizaciones establezcan, por una parte, políticas de seguridad que permitan minimizar el impacto de los ataques y por otra, realicen campañas de concientización a los usuarios sobre el buen uso de los medios tecnológicos, así como sobre las amenazas que existen en el ciberespacio (Naím, 2013). En relación con lo expuesto, las pruebas de penetración (Pentest) en inglés o también llamadas pruebas de intrusión, son una práctica/técnica que consiste en atacar diferentes entornos (un sistema, un servidor o, en general, en una estructura de red,) con la finalidad de encontrar potenciales vulnerabilidades que podrían ser aprovechadas por los ciberdelincuentes. Por lo tanto, el Pentest constituye una herramienta que permite evaluar o auditar sistemas.

2. Marco conceptual

Se puede señalar que la prueba de penetración (Pentest), es un ciberataque simulado contra un sistema informático con la finalidad de descubrir y verificar vulnerabilidades potencialmente explotables, para de esta manera poder mitigar y frustrar ataques avanzados. En este contexto, las metodologías para ejecutar pruebas de penetración surgen como respuesta a la evolución de los sistemas de información, estas metodologías son una guía detallada del proceso de pruebas de penetración, sin embargo, el auditor (pentester) podría encontrarse con diferentes escenarios y dependerá de la información que disponga sobre el elemento a ser auditado, para aplicar tal o cual técnica y esto dependerá de la experiencia del auditor. (Najera-Gutierrez & Ansari, 2018), en el libro Pentesting con Kali Linux 2.0, los entornos y ámbitos en los que se desenvuelven las auditorias seguridades informática engloban varios aspectos que determinan el tipo de auditoría que se llevara a cabo. Entre estas están la auditoría interna y externa.

Auditoría Interna: En la auditoría de seguridad interna o auditoría de caja blanca (White Box), el auditor asume el rol de un usuario que dispone de acceso a los sistemas internos de la empresa y por tanto conoce todas las tecnologías existentes. Además, existe una variante de la auditoría interna conocida como auditoria de caja gris (Gray Box), donde el auditor asume un rol de usuario sin privilegios dentro de la organización. Por lo tanto, la auditoría interna puede ser entonces de caja blanca o de caja gris, en función de los permisos que se tengan (Ortega, 2017).

Auditoría Externa: La auditoría de seguridad externa o auditoría de caja negra (Black Box) asume el rol de un atacante externo a la empresa o hacker que sin el conocimiento de ninguna información previa puede obtener algún beneficio de la organización o, incluso, acceso a información sensible que comprometa la privacidad de la empresa, poniendo a prueba el estado de las barreras de seguridad que dispone la empresa entre Internet y su red corporativa (RUALES CASAL, 2016).

Referente al mismo proceso de pruebas de penetración OSSTMM define seis escenarios, donde se pone de manifiesto las posibles variantes que se podrían encontrar, según la cantidad de información que el auditor disponga sobre el/los objetivos, lo que el objetivo sabe sobre el auditor o espera de la prueba y la legitimidad de la prueba.

Blind: El analista se enfrenta al objetivo sin conocer previamente sus defensas, activos o canales.

Double Blind: El analista se enfrenta al objetivo sin conocer previamente sus defensas, activos o canales.

Gray Box: El analista se enfrenta al objetivo sin conocer previamente sus defensas, activos y con pleno conocimiento de los canales.

Double Gray Box: El analista se enfrenta al objetivo con un conocimiento limitado de sus defensas y activos y con pleno conocimiento de los canales.

Tandem: El analista y el objetivo se preparan para la auditoría, conociendo ambos de antemano todos los detalles de esta.

Reversal: El analista se enfrenta al objetivo con pleno conocimiento de sus procesos y seguridad operativa, pero el objetivo no sabe nada de qué, cómo o cuándo el analista va a realizar la prueba.

Ante la existencia de varios escenarios en los que se pueden aplicar diferentes pruebas de penetración, existen también metodologías y/o frameworks disponibles para este tipo de pruebas y que se detallan a continuación.

2.1 OSSTMM 3

La metodología OSSTMM (Open Source Security Testing Methodology Manual, Manual de código abierto para la realización de pruebas de seguridad) es una medición precisa de la seguridad a nivel operacional, lo cual evita suposiciones y evidencia anecdótica. Como una metodología, está diseñada para ser consistente y repetible. Se fundamenta en saber y medir que tan bien funciona la seguridad de una empresa. (Díaz Barrera, 2018). Maucaylle (2019), menciona que las auditorías de seguridad que utilizan una metodología OSSTMM obtienen una compresión profunda de la interconexión de las cosas, ya que la versión 3 de OSSTMM abarca todos los canales, humano, físico, inalámbrico, telecomunicación y redes de datos, agrupados en tres clases (seguridad física PHYSSEC, seguridad del espectro inalámbrico SPECSEC, seguridad de las comunicaciones COMSEC), por lo tanto, propone que se ejecute pruebas sobre cada canal. OSSTMM proporciona descripciones específicas para las pruebas de seguridad operativa sobre todos los canales operativos, que incluyen redes humanas, físicas, inalámbricas, de telecomunicaciones y de datos, sobre cualquier vector, y la descripción de las métricas derivadas.

El flujo de trabajo de esta metodología inicia con una revisión de la postura del objetivo, conociendo los requisitos operativos y finaliza con la comparación de los resultados, es decir que se trata de un proceso cíclico completo (canal, módulo, tarea) en el que el primer paso es la revisión de requisitos operativos que permitan interactuar con el objetivo, y el último paso es la revisión y comparación de los hallazgos con cualquier alarma, alerta, informe o registro de acceso. En resumen: sabes lo que tienes que hacer, lo haces y luego compruebas lo que has hecho (Bocardo, 2006).

Mena (2021) el ciclo empleado por OSSTMM, es jerárquico y menciona en primer lugar al canal, que es el medio de interacción; los módulos que son las propiedades que se aplican al canal y que son comunes para todos ellos; y por último las tareas que son las acciones que se realizan para cada módulo. Para continuar es necesario tener en cuenta ciertos conceptos alineados a esta metodología:

Visibilidad: es un medio que permite calcular la oportunidad. Hace referencia a los activos que se pueden identificar, por ende, si un activo no es descubierto, no existe la probabilidad de que pueda ser atacado.

Acceso: Dado que la seguridad es la separación de una amenaza y un activo, el

acceso se refiere a la capacidad de interactuar con el activo directamente. El acceso se calcula por el número de lugares diferentes en los que puede producirselainteracción.

Confianza: relación que existe entre objetivos, donde se acepta la interacción libre entre ellos. Aunque la confianza puede ser un agujero de seguridad, es un sustituto común de la autenticación y un medio para evaluar las relaciones de una manera racional y repetible.

Es esencial que el auditor elija el tipo de prueba adecuado, en función de la minuciosidad, la actividad, el tiempo asignado y los requisitos de la auditoría, por lo que, para la ejecución de pruebas de penetración, esta metodología consta de 4 fases y 17 módulos:

A. Fase deInducción:
A.1 Revisión de la postura
A.2 Logística
A.3 Verificaciónde la detección activa

En la fase de inducción, el analista comienza la auditoríaconlacomprensióndelosrequisitos dela misma,elalcanceylaslimitacionespara laauditoría de este alcance. A menudo, el tipo de prueba se determina mejor después de esta fase.

B. Fase deInteracción:
B.4 Auditoríadevisibilidad
B.5 Verificación del acceso
B.6 Verificación de la confianza
B.7 Verificación delcontrol

En la fase de interacción se definirá el alcance. El núcleo de la prueba de seguridad básica requiere conocer el alcance en relación con las interacciones con los objetivos transmitidos a las interacciones con los activos.

C. Fase deInvestigación:
C.8 Verificación delproceso
C.9 Verificación de la configuración / Verificación de la formación
C.10 Validación de la propiedad
C.11 Revisión de la segregación
C.12 Verificación de la exposición
C.13 Exploración de Inteligencia Competitiva

En la fase de investigación se sacan a la luz los distintos tipos de valor o el perjuicio de la información extraviada y mal gestionada como activo. Gran parte de la auditoría de seguridad tiene que ver con la información que el analista descubre.

D. Fase deIntervención:
D.14 Verificación de la cuarentena
D.15 Auditoría deprivilegios
D.16 Validación de la capacidad de supervivencia/Continuaddelservicio
D.17 Revisión de alertas y registros / Encuesta final

La fase de intervención suele ser la fase final de una prueba de seguridad para asegurar que las interrupciones no afecten a las respuestas de las pruebas menos invasivas y porque la información para realizar estas pruebas puede no conocerse hasta que se hayan realizado otras fases. Estas pruebas se centran en los recursos que los objetivos requieren en el ámbito, los mismos que pueden ser cambiados, sobrecargados o privados para causar una penetración o una interrupción.

En general las auditorías de seguridad buscan establecer el estado actual la seguridad de una organización, a fin de poder definir las medidas que se deben adoptar frente a las amenazas encontradas, en este contexto, OSSTMM incluye el concepto Risk Assessment Values (RAV) por sus siglas en inglés, el cual permite identificar el estado actual de seguridad de la superficie de ataque. El RAV es una medida a escala de la superficie de ataque, es decir, que posibilita tener una estadística y realizar seguimiento del comportamiento que ha tenido la seguridad de la organización a través del tiempo (Castro Vasquez, 2019). El RAV no mide el riesgo de una superficie de ataque, sino que permite medirla. No puede predecir si un objetivo concreto será atacado, pero sí puede indicar en qué parte del objetivo será atacado, de qué tipos de ataques puede defenderse con éxito el objetivo, a qué profundidad puede llegar un atacante y cuánto daño puede causar, logrando de esta manera evaluar las

confianzas (y los riesgos) con mucha más precisión. Para emplear esta métrica, se debe evitar datos imprecisos y relativos que pretende encontrar los componentes mínimos requeridos, es por eso que el RAV propone 3 elementos que permiten evaluar la superficie de ataque: porosidad, controles y limitaciones (Sánchez Robayo, 2012). Según (Boudreaux, 2003) la representación del RAV es similar a cómo la gente utiliza los porcentajes, ya que se calcula con un logaritmo de base 10, lo que hace una representación más comprensible. Es extremadamente flexible, por lo que se puede comparar múltiples superficies de ataque incluso si el ámbito o los objetivos son muy diferentes: el 95% de RAV de un ámbito con 1.000 sistemas informáticos es comparable al 95% de RAV con sólo 10 sistemas, que puede compararse de nuevo con un edificio con un 95% de RAV. Los tres ejemplos proporcionarán la misma información a una persona de que la protección del objetivo es un 5% deficiente y, portanto, está expuesta a un ataque. Saber qué interacciones requieren menos equilibrio que otras es una cuestión de saber en qué interacciones debemos confiar. Para las operaciones en las que tenemos menos razones para confiar, debemos aplicar más de los diez controles para conseguir un equilibrio perfecto.

2.2. PTES.

Ortiz Castillo (2020) el proyecto PTES (Penetration Testing Execution Standard) surgió a principios del año 2009 y se encuentra en la versión 1.0; fue diseñado para ofrecer a las empresas y proveedores de servicios un lenguaje y enfoque común para realizar pruebas de penetración. Este estándar consta de 7 fases, las mismas que cubren todo lo relacionado con una prueba de penetración, desde la

2.2.1 Pre-engagement Interactions o interacciones previas al compromiso

El objetivo de esta etapa es establecer reglas claras para la ejecución de la prueba de penetración donde se define el alcance, que es posiblemente uno de los componentes más importantes de una prueba de penetración, pero también es uno de los que más se pasa por alto. Antes de comenzar una prueba de penetración, se deben identificar todos los objetivos. Los objetivos pueden ser proporcionados por el cliente en forma de direcciones IP específicas, rangos de red o nombres de dominio. En algunos casos, el único objetivo que proporciona el cliente es el nombre de la organización y espera que los evaluadores puedan identificar el resto por sí mismos. Además, es importante definir si los sistemas como firewalls e IDS / IPS o equipos de red que se encuentran entre el auditor y el objetivo final también forman parte del alcance. Este proceso resulta importante a la hora de establecer las expectativas del cliente y así entender cuáles son los resultados esperados (Areitio Bertolín, 2008).

2.2.2 Intelligence Gathering o recolección de información

PTES plantea tres niveles de recolección de información:

N1: (Impulsado por el cumplimiento) Obtención de información mediante herramientas automatizadas disponibles, apropiado para cumplir con el requisito de cumplimiento.

N2: (Mejores prácticas) Este nivel se puede crear utilizando herramientas automatizadas del N1 más el análisis manual. Una buena comprensión del negocio, incluida información como la ubicación física, las relaciones comerciales, el organigrama, etc.

N3: incluye toda la información del N1 y N2 junto con el análisis riguroso, comprensión profunda de las relaciones comerciales, lo que implica la inversión de gran cantidad de horas para lograr la recopilación y la correlación.

Cuanta más información pueda recopilar durante esta fase, más vectores de ataque podrá utilizar en el futuro (Ortiz Castillo, 2020).

2.2.2 Threat Modeling o modelamiento de amenazas:

PTES no usa un modelo específico, sino que requiere que el modelo usado sea consistente en términos de su representación de amenazas, sus capacidades, sus calificaciones según la organización que se está probando y la capacidad de ser aplicado repetidamente a pruebas futuras con los mismos resultados (Cruz & Fernández, 2012).

Cada uno se divide, respectivamente, en activos y procesos comerciales y las comunidades de amenazas y sus capacidades.

Proceso de modelado de amenazas de alto nivel

- Reúna la documentación relevante
- Identificar y categorizar activos primarios y secundarios.
- Identificar y categorizar amenazas y comunidades de amenazas
- Mapear comunidades de amenazas contra activos primarios y secundarios

2.2.3 Vulnerability Analysis o análisis de vulnerabilidades:

Gómez (2018) dice el análisis de vulnerabilidades es el proceso que permite detectar fallas en sistemas y aplicaciones que pueden ser aprovechadas por un atacante. Estas brechas de seguridad varían desde una mala configuración de un servidor y/o servicio, hasta un diseño de aplicación inseguro. En este sentido, el evaluador debe analizar adecuadamente el alcance de las pruebas en cuanto a la profundidad (la ubicación de una herramienta de evaluación, requisitos de autenticación) y amplitud (redes de destino, segmentos, hosts, aplicaciones, inventarios, entre otros) aplicables para cumplir con los objetivos y/o requisitos del resultado deseado.

En esta etapa se pueden ejecutar pruebas activas y pasivo; las pruebas activas implican la interacción directa con el componente que se está probando para detectar vulnerabilidades de seguridad. Existen dos formas distintas de interactuar con el componente de destino: automática y manual; las pruebas pasivas en cambio, se basan en el análisis de metadatos de archivos expuestos. Estos podrían contener direcciones internas y rutas a servidores, direcciones IP internas y otra información que un evaluador podría usar para obtener acceso o información adicional.

2.2.4 Exploitation o explotación

La fase de explotación de una prueba de penetración se centra únicamente en establecer el acceso a un sistema o recurso evitando las restricciones de seguridad. El enfoque principal es identificar el principal punto de entrada a la organización e identificar los activos objetivo de alto valor, que debieron haberse obtenido en la fase de análisis de vulnerabilidades. En última instancia, el vector de ataque debe tener en cuenta la probabilidad de éxito y el mayor impacto en la organización (Chique Velasquez, 2021).

2.2.5 Post Exploitation o Post explotación

Herrera, (2019) El propósito esta fase es determinar el valor de la máquina comprometida y mantener el control de la misma para su uso posterior. El valor de la máquina está determinado por la sensibilidad de los datos almacenados en ella y la utilidad para comprometer aún más la red, además el evaluador podrá identificar y documentar datos confidenciales, ajustes de configuración, canales de comunicación y relaciones con otros dispositivos de red que se pueden usar para obtener más acceso a la red; cabe señalar que este proceso se realiza sin llevar a cabo ninguna actividad injustificada que ponga en riesgo a la organización.

2.2.6 Reporting o presentación de reporte

PTES no proporciona un formato específico para la presentación de reportes, sin embargo, propone 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. El informe debe comunicar los objetivos, métodos y resultados de las pruebas realizadas a diversas audiencias. Para lo cual se definen dos partes: resumen ejecutivo y reporte técnico (Fernández Díaz,2003).

El resumen ejecutivo: comunicará al lector los objetivos específicos de la prueba de penetración y los resultados de alto nivel del ejercicio de prueba. Está dirigido a aquellos que estén a cargo de la supervisión y visión estratégica del programa de seguridad, así como cualquier miembro de la organización que pueda verse afectado por las amenazas identificadas /confirmadas.

Reporte técnico: Esta sección comunicará al lector los detalles técnicos de la prueba y todos los aspectos/componentes acordados como indicadores clave de éxito dentro del ejercicio previo a la participación. La sección del informe técnico describirá en detalle el alcance, la información, la ruta del ataque, el impacto y las sugerencias de remediación de la prueba.

2.3 OWASP

The Open Web Application Security Project (OWASP) es un proyecto enfocado a la seguridad de las aplicaciones web y ofrece un marco de referencia para ejecutar pruebas de penetración, alineadas al ciclo de vida del software. (Miranda Ari, 2016) redacta la comprobación o testing es un proceso de comparación del estado de algo ante un conjunto de criterios. En la industria de la seguridad, a menudo se realizan pruebas contra un conjunto de criterios mentales que no están ni bien definidos ni completos. OWASP ha sido diseñado para ayudar a las organizaciones a entender qué comprende la realización de un programa de pruebas, y ayudarlas a identificar los pasos necesarios a realizar para construir y operar dicho programa de pruebas sobre sus aplicaciones web.

Un programa de pruebas efectivo debería tener componentes que comprueban:

- Las Personas: para asegurarse de que hay la educación y concienciación adecuadas.
- Los Procesos: para asegurarse que hay las políticas y estándares adecuados y que las personas saben cómo seguir dichas políticas.
- La Tecnología: para asegurarse de que el proceso ha sido efectivo en su implementación

Girón Miranda & Torres Roa (2015); una clasificación de amenaza y contramedida que tenga en cuenta las causas profundas de las vulnerabilidades es el factor crítico para verificar que los controles de seguridad están diseñados, codificados, y construidos de tal manera que el impacto debido a la exposición de tales vulnerabilidades sea mitigado. En el caso de las aplicaciones web, la exposición de

los controles de seguridad para vulnerabilidades comunes, como el OWASP Top Ten, puede ser un buen punto de partida para obtener los requerimientos de seguridad generales. Este marco de pruebas consta de las siguientes actividades que deberían tener lugar:

Figura 1

Flujo de trabajo del entorno de pruebas OWAS

Flujo de trabajo del entorno de pruebas OWASP	
Antes del desarrollo	-Revision del proceso de SDLC -Revision de la política -Revision de estándares
Definicion y diseño	-Revision de requerimientos -Revisión de arquitectura y diseño -Crear / revisar modelos UML -Crear/revisar modelos de amenazas
Desarrollo	-Revisión de código -Inspecciones de código por fases -Pruebas de sistema y unidad
Instalación	-Pruebas de intrusión -Revisiones de gestión de configuración -Pruebas de sistema y unidades -Pruebas de aceptación
Mantenimiento	-Verificación decambios -Revisiones deintegridad -Revisiones de gestion operativa -Pruebas de regresión

Elaboración propia

2.3.1 Prueba de intrusión a aplicaciones web

Una prueba de intrusión de aplicación web está enfocada únicamente a evaluar la seguridad de una aplicación web, proceso que conlleva un análisis activo de la aplicación en busca de cualquier debilidad, fallos técnicos o vulnerabilidades; cualquier hallazgo será presentado al propietario del sistema, junto con una evaluación de su impacto, y a menudo con una propuesta para su mitigación o una solución técnica. La metodología de pruebas de intrusión de aplicación web OWASP se basa en un enfoque / acercamiento de caja negra (Zapata, 2019).

El modelo de pruebas consta de:

- Auditor: La persona que realiza las actividades de comprobación.
- Herramientas y metodología: El núcleo de este proyecto de guía de pruebas.
- Aplicación: La caja negra sobre la que realizar las pruebas.

Según la metodología OWASP, las pruebas de intrusión se dividen en 2 fases: Modo pasivo: el evaluador intenta comprender la lógica de la aplicación, juega con la aplicación; puede usarse una utilidad para la recopilación de información, como un proxy HTTP, para observar todas las peticiones y respuestas HTTP. Al final de esta fase esta persona debería comprender cuales son todos los puntos de acceso (puertas) de la aplicación (p.e. cabeceras HTTP, parámetros, cookies). Modo activo: en esta fase el evaluador empieza a realizar las pruebas usando la metodología descrita en los siguientes apartados:

- Pruebas de gestión de la configuración
- Pruebas de la lógica de negocio
- Pruebas de Autenticación
- Pruebas de Autorización
- Pruebas de gestión de sesiones
- Pruebas de validación de datos
- Pruebas de denegación de Servicio
- Pruebas de Servicios Web
- Pruebas de AJAX 66,9
- 56,7

2.3.2 Redacción de informes: Valorar el riesgo real

Descubrir vulnerabilidades es importante, pero igualmente importante es ser capaz de estimar el riesgo asociado para el negocio. La

idea es crear una metodología general para descomponer los hallazgos de seguridad y evaluar los riesgos con el objetivo de priorizarlos y gestionarlos. En la tabla propuesta anteriormente se puede representar con facilidad una captura del proceso de evaluación en un momento dado. Esta tabla representa la información técnica que debe ser entregada al cliente, por lo que es importante presentar un resumen ejecutivo para la gerencia (García Münzer, 2005). Finalmente, con la información completa se procede a redactar el informe (ejecutivo y técnico), donde vamos a sintetizar todos los hallazgos, y en la tabla incluiremos, un número identificador, los elementos afectados, una descripción técnica, una sección sobre cómo resolver la incidencia, el nivel de riesgo y el valor de impacto (Montalván Dávila,2018).

3 Métodos

Para la elaboración del presente estudio, se revisaron varias fuentes bibliográficas, trabajos de investigación sobre las diferentes metodologías y estándares existentes para la ejecución de pruebas de penetración. En este contexto se investigó sobre las metodologías más utilizadas por los profesionales de la seguridad informática, como son OSSTMM, PTES y OWASP. Cada una con sus particularidades cuyo objetivo es el mismo, alcanzar niveles de seguridad aceptables.

4 Herramientas

Con el afán de lograr la eficiencia durante la ejecución de las pruebas de penetración, a continuación, se describen varias herramientas que permiten automatizar algunas de las tareas que realiza el evaluador:

- Nmap: Utilidad multi plataforma de código abierto con licencia GNU para descubrimiento de redes y auditoria de seguridad, que permite determinar si un host está disponible en la red, los servicios activos, el sistema operativo y los filtros que tiene el firewall.

- Zenmap: brida una interfaz gráfica Nmap. Se puede decir que es un cliente que se utiliza para simplificar su uso sin perder su poder. Su licenciamientoesdesoftwarelibre.

- Nexpose: Tiene una licencia propietaria de pago. Es una herramienta que permite hacer un análisis exhaustivo de las vulnerabilidades de ambientes y redes.LaversióngratuitadeNexpose está limitada a 32 direcciones IP a la vez, y debe volver a aplicar después de un año y esta soportada por Rapid 7

- Nessus: Tiene una licencia propietaria de pago. Es una solución de evaluación de vulnerabilidad estándar de la industria que ayuda a identificar vulnerabilidades, incluyendo fallas de software, parches faltantes, malware y configuraciones erróneas, en una variedad de sistemas operativos, dispositivos y aplicaciones.

- OpenVas: Su licenciamiento es GNU GPL. Es un Software de escaneo de vulnerabilidades muy completo, optimizado para pruebas a gran escala, dentro de sus características están: realizar pruebas no autenticadas y pruebas autenticadas; además, cuenta con su propio lenguaje para implementar cualquier tipodepruebadevulnerabilidad.

- Foca: Es una herramienta para encontrar metadatos e información oculta en documentos de texto y hojas de cálculo, etc. Realiza una revisión completa de los ficheros para obtener datos relevantes de una empresa. Es una herramienta que se

emplea de forma recurrente durante la etapa de recolección de información.

- Metasploit: Framework con licencia BDS. Permite desarrollar y ejecutar exploit contra maquinas remotas. Se construyo inicialmente en leguaje Perl, pero fue reescrito en Ruby; está orientado al desarrollo y ejecución de exploit contra maquinas remotas. La versión no paga tiene soporte de la comunidad y la versión paga conocida como Metasploit pro esta soportada por Rapid7.

- OWASP-ZAP: Una de las herramientas más potentes del programa OWASP es ZAP (Zed Attack Proxy). Esta plataforma está diseñada especialmente para monitorizar la seguridad de las aplicaciones web, siendo una de las aplicaciones del proyecto más activas en cuanto a auditorías de seguridad. Herramienta totalmente gratuita y de código abierto, multi-plataforma, compatible incluso con Raspberry Pi, fácil de instalar, soportada por una gran comunidad a nivel mundial.

- Wireshark: es un software de código abierto bajo la licencia GNU GPL. Esta aplicación es un analizador de paquetes y protocolos, capaz de registrar absolutamente todos los paquetes que pasan por una red, inclusive es capaz de descifrar los paquetes enviados a través de los principales protocolos de conexión segura para poder analizar sin problema su contenido.

- Kali Linux: es una distribución basada en Debian GNU/Linux diseñada principalmente para la auditoría y seguridad informática en general. Kali Linux es la versión actualizada y optimizada de la distro BackTrack desarrollada por Offensive Security. Dentro de Kali podemos encontrar un total de 600 aplicaciones de hacking y seguridad, entre las que podemos destacar: Nmap, Wireshark, John the Ripper, Aircrack-ng, THC Hydra, Nessus, Metasploit.

5 Discusión

Las metodologías presentadas constituyen un marco de referencia para le ejecución de pruebas de penetración, las mismas que buscan dar una pauta para realizar dichas pruebas, sin embargo, cada una de ellas tiene un enfoque particular, aspecto que se debe tener en cuenta a la hora de elegir que metodología implementar en una organización, lo cual va a depender de los resultados que se esperan y de la experiencia del auditor. El auditor por su parte puede, basado en los lineamientos propuestos por cada metodología, puede definir su propia estructura, para realizar las pruebas de penetración.

Es evidente que existen marcadas diferencias entre las metodologías expuestas, sin embargo, todas siguen una estructura general que consiste en entender el entorno en el que se va a ejecutar las pruebas de penetración, interactuando con el/los objetivos y conociendo el sistema en busca de vulnerabilidades, explotarlas de ser el caso y finalmente elaborar y presentar un informe que muestre el proceso realizado, identificando todos los hallazgos, explicando hasta donde se puede llegar si las vulnerabilidades son explotadas y lo más importante las recomendaciones para cerrar esas brechas de seguridad que ponen en riesgo a la organización. Las pruebas de penetración muestran la imagen real de la amenaza existente, porque se pone a prueba la fiabilidad de las medidas y herramientas de ciberseguridad con las que cuenta la organización, además podemos comprobar los efectos reales de

un ciberataque a nuestro sistema informático y medir qué capacidad de reacción tendría la empresa en caso de producirse. La realización de un pentest de forma periódica determinará los recursos técnicos, la infraestructura, el arsenal físico y de personal que contienen aspectos débiles que requieren desarrollo y mejora.

6. Referencias

Areitio Bertolín, J. (2008). *Seguridad de la información. Redes, informática y sistemas de información*. Editorial Paraninfo.

Bocardo, R. (2006). *Creatividad en la ingeniería de diseño*. Equinoccio.

Boudreaux, K. (2003). *Finanzas*. Gran Bretaña: Edinburgh Business School.

Castro Vasquez, C. A. (2019). *Pruebas de penetración e intrusión*.

Chique Velasquez, W. F. (2021). *Prueba de penetración en la seguridad de la información de la empresa Electro Puno SAA*.

Cruz, A. M., & Fernández, M. A. (2012). Propuesta Integral de un Modelo de Gestión por Procesos de Negocio (PIM-GPN). *México DF: Instituto Politécnico Nacional*.

Cubillo Arribas, J. (2014). *ARLE: una herramienta de autor para entornos de aprendizaje de realidad aumentada*.

Díaz Barrera, E. R. (n.d.). *Análisis de metodologías para pruebas de penetración mediante Ethical Hacking*.

Fernández Díaz, N. (2003). La violencia sexual y su representación en la prensa. *La Violencia Sexual y Su Representación En La Prensa*, 1–255.

García Münzer, D. G. (2005). *Aplicación de modelos de decisión y evaluación de riesgo en exploración, perforación y explotación de petróleo*.

Girón Miranda, L. A., & Torres Roa, H. A. (2015). *Detección y generación de recomendaciones para el cierre de las vulnerabilidades relacionadas en el top 10 OWASP identificadas en la aplicación web de historias clínicas en la institución prestadora de servicios de salud especializada en audiología Audioc*. Universidad Piloto de Colombia.

Gómez Mojica, Y. M. (2018). *Estudio de seguridad en bases de datos SQL y NOSQL.*

Martín Herrera, A. (2019). *Laboratorio de Pentesting con GNS3*.

Maucaylle Leandres, A. (2019). *Construcción de un modelo de red virtual para aplicar técnicas de hacking ético y poder analizar los eventos relacionados a la seguridad informática sobre una infraestructura virtual*.

Mena Asprilla, O. E. (n.d.). *Análisis de riesgo de seguridad en los dispositivos móviles personales con sistema operativo android.*

Miranda Ari, M. (n.d.). *Automatización en el control de la información de productos para la empresa TECNOALIMENTOS LTDA.*

Montalván Dávila, F. A. (2018). *Efecto de la regulación de telecomunicaciones sobre el crecimiento del indicador de desarrollo de las tecnologías de la información y comunicación–TIC en el Perú*.

Naím, M. (2013). *El fin del poder: Empresas que se hunden, militares derrotados, papas que renuncian, y gobiernos impotentes: cómo el poder ya no es lo que era*. Debate.

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

Ortega, A. S. M. (2017). *Metodología de Hacking Ético para Instituciones Financieras, aplicación de un caso práctico*. UNIVERSIDAD DE CUENCA.

Ortiz Castillo, A. M. (2020). *Introducción a las pruebas de penetración*.

Perrenoud, P. (1990). *La construcción del éxito y del fracaso escolar: hacia un análisis del éxito, del fracaso y de las desigualdades como realidades construidas por el sistema escolar*. Ediciones Morata.

Phillips, P. (2019). *Megacapitalistas: la élite que domina el dinero y el mundo*. Roca Editorial.

Recalde Caicedo, J. P. (2019). *Plan de implementación de un SGSI y aplicación de controles críticos en el centro de operaciones de seguridad en la empresa GMS*. Quito, 2019.

Sánchez Robayo, O. M. (2012). *Hacking*

ético para el centro de operación de la red para la zona 8 de la Empresa CNT con software de código abierto. Quito: Universidad de las Américas, 2012.

Zapata, J. (2019). *Uso de tecnologías de pruebas de penetración para validación de seguridad de aplicaciones web basado en el top 10 de vulnerabilidades de OWASP*.