ANALISIS DE VULNERABILIDADES Y ESTRATEGIAS DE CONTINGENCIA EN SERVIDORES DE ENTIDAD FINANCIERA

JAIR ANDRÉS RODRÍGUEZ VALDERRAMA

UNIVERSIDAD SANTO TOMAS DE AQUINO

FACULTAD DE INGENIERIA

INGENIERIA DE TELECOMUNICACIONES

BOGOTÁ D.C

2023

ANALISIS DE VULNERABILIDADES Y ESTRATEGIAS DE CONTINGENCIA EN SERVIDORES DE ENTIDAD FINANCIERA

Presentado por:

JAIR ANDRES RODRIGUEZ VALDERRAMA

Trabajo opción de grado Pasantías para optar por el título de Ingeniero de Telecomunicaciones

Tutor: Pedro Alejandro Mancera Lagos

Ingeniero Electrónico

UNIVERSIDAD SANTO TOMAS DE AQUINO

FACULTAD DE INGENIERIA

INGENIERIA DE TELECOMUNICACIONES

BOGOTÁ D.C

2023

RECTOR GENERAL

Padre José Gabriel Mesa Angulo, O.P.

VICERRECTOR ADMINISTRATIVO Y FINANCIERO GENERAL

Padre, Wilson Mendoza Rivera, O.P.

VICERRECTOR ACADÉMICO GENERAL

P. Eduardo Gonzáles Gil, O.P

SECRETARIA GENERAL

Ingrid Lorena Campos Vargas

SECRETARIA DE DIVISIÓN

E. C. Luz Patricia Rocha Caicedo

DECANO FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES

Nota de Aceptación.

_____

_____

_____

_____

_____

Firma Ingeniero. Pedro Alejandro Mancera Lagos

Tutor Asignado

_____

Firma del Jurado

_____

Firma del Jurado

_____

Fecha

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

RESUMEN

En la actualidad, los bancos le apuestan enormemente a su área de TI para lograr un crecimiento empresarial cada vez mayor. La importancia de la detección de vulnerabilidades y las estrategias de contingencia ante cualquier ataque, obligan a implementar metodologías para identificar vulnerabilidades y ejecutar acciones de contingencia. En el presente trabajo, se realiza un análisis de las distintas metodologías existentes, y aplicamos en un entorno diseñado, la más adecuada para las necesidades del banco, donde se realizó la pasantía.

ABSTRACT

The bank we will talk about throughout this monograph is a very well-known bank in Colombia (For security and confidentiality reasons, this paper abstains from mentioning the name of the entity). Belonging to the Aval group and being managed by one of the richest men in the country, this bank has built a reputation over the years. Famous for the services it provides, such as savings accounts, loans and cards (among others), this bank is betting heavily on its IT area to achieve ever-increasing business growth. In this part, the important area of cybersecurity is implicit, which, being a financial institution, needs to be very cautious to avoid attacks and hacks that put its capital and that of its customers at risk. Therefore, this paper will present a possible implementation of a model which will be useful to strengthen their cybersecurity.

INTRODUCCIÓN

En la era contemporánea, con el auge de la era digital, las empresas del mundo casi que en su totalidad han tenido que adaptarse a esta, y el sector bancario y financiero no es la excepción.

Todos los bancos en la actualidad manejan su información de manera digital, lo cual los vuelve un blanco vulnerable ante hackeos y ataques cibernéticos con el objetivo de robar su información y la de sus clientes, con el simple objetivo de robarles dinero.

Es por esto, que los bancos tienen toda un área enfocada a la ciberseguridad, que recauda y analiza los datos de los servidores donde los bancos almacenan su información, escaneando constantemente en busca de intrusos y/o amenazas en que pongan en riesgo los datos de la compañía.

Además de esto, estos equipos de ciberseguridad son los encargados de establecer medidas, tanto preventivas como de emergencia ante posibles ciber ataques.

Dentro de esta monografía veremos como la importancia del área de ciberseguridad de la entidad financiera para poder identificar y prevenir y/o solventar estas amenazas.

OBJETIVOS

OBJETIVO GENERAL: Realizar un análisis que permita identificar posibles amenazas para los servidores de una entidad financiera.

OBJETIVOS ESPECÍFICOS:

- Identificar las distintas metodologías de evaluación de amenazas, análisis y gestión de riesgos.
- Plantear una propuesta de implementación de una de estas metodologías para la entidad financiera.
- Identificar vulnerabilidades y acciones de contingencia.

PLANTEAMIENTO DEL PROBLEMA

En la actualidad, el uso de tecnologías de la información en el sector bancario es fundamental para garantizar la eficiencia en los servicios que se ofrecen a los clientes. Sin embargo, esta dependencia de la tecnología también conlleva un mayor riesgo de vulnerabilidades y amenazas cibernéticas, que pueden afectar la seguridad de los datos y la confidencialidad de la información.

El Banco, como entidad financiera, enfrenta diversos riesgos cibernéticos, incluyendo acceso no autorizado a datos, propagación de malware, vulnerabilidades de software y compromiso de sistemas de seguridad. La seguridad de sus servidores es crucial debido al almacenamiento y procesamiento de información financiera y personal de los clientes. Por tanto, es fundamental realizar un análisis de vulnerabilidades para identificar y mitigar riesgos en los servidores. Un gran riesgo es la falta de una configuración adecuada de los firewalls, lo que permite acceso no autorizado y exposición de información confidencial a amenazas externas. Además, la falta de actualizaciones de seguridad podría dejar a los servidores expuestos a vulnerabilidades conocidas. La protección efectiva de la infraestructura del Banco es vital para salvaguardar la confianza de los clientes y proteger su información sensible.

Además, este proyecto también contribuirá a mejorar la imagen y reputación del Banco al demostrar su compromiso con la seguridad y privacidad de los datos de sus clientes. En un mundo cada vez más conectado y digitalizado, los clientes confían en que sus datos están protegidos y seguros. Al invertir en un proyecto de análisis de vulnerabilidades, el Banco demuestra su compromiso con la seguridad y la privacidad de los datos de sus clientes, lo que puede aumentar la confianza y lealtad de los clientes hacia la organización.

Por lo tanto, se requiere un proyecto de análisis de vulnerabilidades en los servidores del Banco, que tenga como objetivo identificar y corregir las vulnerabilidades de seguridad existentes en los firewalls y otros componentes de los sistemas. Esto permitirá mejorar la seguridad de los servidores, minimizar el riesgo de exposición de datos confidenciales y garantizar la protección de los activos de la entidad financiera.

Se plantea entonces la siguiente pregunta "¿Qué medidas puede tomar esta entidad financiera de cara a estos riesgos latentes?"

Una vez identificadas las vulnerabilidades, se deben tomar medidas para mitigar los riesgos. Esto puede incluir la actualización de los firewalls, la aplicación de parches de seguridad en los sistemas operativos y aplicaciones, la configuración de nuevas reglas de acceso y filtrado de tráfico, la implementación de controles de acceso más estrictos, y la educación y concienciación de los empleados sobre las buenas prácticas de seguridad informática.

Podemos decir entonces que el proyecto de análisis de vulnerabilidades en los servidores del Banco tiene como objetivo identificar y mitigar los riesgos de seguridad en los sistemas de la entidad financiera, con un enfoque particular en la configuración de los firewalls y otros componentes críticos. Al realizar este proyecto, se puede mejorar la seguridad de los servidores, minimizar el riesgo de exposición de datos confidenciales y garantizar la protección de los activos de la entidad financiera.

ALCANCE

El proyecto de análisis de vulnerabilidades en los servidores del Banco tiene como objetivo identificar y mitigar los riesgos de seguridad en los sistemas de la entidad financiera, con un enfoque particular en la configuración de los firewalls y otros componentes críticos. El proyecto se desarrollará en varias etapas, incluyendo la evaluación de los firewalls, la revisión de la configuración de los sistemas operativos y aplicaciones, la evaluación de las políticas y procedimientos de seguridad, y las pruebas de penetración.

Para lograr los objetivos del proyecto, se llevarán a cabo las siguientes actividades:

Evaluación de los firewalls del Banco: se revisará la configuración de los firewalls, incluyendo las políticas de acceso y las reglas de filtrado de tráfico, para identificar posibles vulnerabilidades y brechas en la seguridad.

Revisión de la configuración de los sistemas operativos y aplicaciones: se evaluará la configuración de seguridad de los sistemas operativos y aplicaciones que se ejecutan en los servidores del Banco, incluyendo la presencia de parches de seguridad y actualizaciones, y la presencia de configuraciones predeterminadas que puedan ser explotadas por los atacantes.

Evaluación de las políticas y procedimientos de seguridad: se revisarán las políticas y procedimientos de seguridad del Banco, incluyendo las políticas de gestión de contraseñas, la política de respaldo de datos y la política de uso de dispositivos móviles, para evaluar la efectividad de las medidas de seguridad existentes y detectar posibles debilidades.

Pruebas de penetración: se realizarán pruebas de penetración para evaluar la resistencia del sistema a los ataques y simular situaciones de riesgo. Esto incluirá la simulación de ataques de fuerza bruta, la explotación de vulnerabilidades de software, y la evaluación de la seguridad de los datos transmitidos a través de la red.

Mitigación de vulnerabilidades: una vez identificadas las vulnerabilidades, se tomarán medidas para mitigar los riesgos. Esto puede incluir la actualización de los firewalls, la aplicación de parches de seguridad en los sistemas operativos y aplicaciones, la configuración de nuevas reglas de acceso y filtrado de tráfico, la implementación de controles de acceso más estrictos, y la educación y concienciación de los empleados sobre las buenas prácticas de seguridad informática.

El proyecto se llevará a cabo en un plazo de seis meses y se llevará a cabo por un equipo de expertos en ciberseguridad. El equipo incluirá expertos en firewalls, sistemas operativos, aplicaciones, políticas y procedimientos de seguridad, y pruebas de penetración. El equipo también trabajará en colaboración con el personal de TI del Banco para asegurar que todas las medidas de seguridad se apliquen de manera efectiva y sin interrupciones en los servicios del banco.

Al finalizar el proyecto, se presentará un informe detallado de las vulnerabilidades identificadas y las medidas tomadas para mitigar los riesgos. El informe incluirá recomendaciones para mejorar la seguridad de los sistemas y garantizar la protección de los activos del Banco. Además, se proporcionará una sesión de capacitación a los empleados del Banco para concienciarlos sobre las buenas prácticas de seguridad informática y cómo pueden contribuir a proteger los sistemas y datos del banco.

El alcance del proyecto se limita a los servidores del Banco y no incluye la evaluación de la seguridad de los sistemas en línea ni de los servicios de terceros utilizados por el banco. Además, el equipo de seguridad de la entidad financiera colaborará activamente en el proyecto y proporcionará acceso a los sistemas y datos necesarios para realizar las pruebas y evaluaciones.

Es importante destacar que la finalidad del proyecto no es atacar el sistema del Banco, sino identificar posibles vulnerabilidades y ayudar al banco a mitigar los riesgos de seguridad. Todas las actividades se llevarán a cabo de manera ética y en cumplimiento con las leyes y regulaciones aplicables.

Así entonces, el proyecto de análisis de vulnerabilidades en los servidores del Banco es una iniciativa clave para garantizar la seguridad de los activos del banco y proteger la confidencialidad, integridad y disponibilidad de los datos de sus clientes. El proyecto se desarrollará en varias etapas y se llevará a cabo por un equipo de expertos en ciberseguridad, con la colaboración activa del personal de TI del Banco. Al finalizar el proyecto, se presentará un informe detallado de las vulnerabilidades identificadas y las medidas tomadas para mitigar los riesgos, así como una sesión de capacitación para concienciar a los empleados sobre las buenas prácticas de seguridad informática.

JUSTIFICACION

La justificación del proyecto de análisis de vulnerabilidades en los servidores del Banco radica en la necesidad de proteger los datos de los clientes y de la organización de los posibles riesgos de seguridad informática. En la actualidad, los sistemas informáticos de las empresas son cada vez más complejos y sofisticados, y por lo tanto, más propensos a sufrir vulnerabilidades de seguridad.

El Banco maneja una gran cantidad de información sensible y confidencial de sus clientes, como datos personales, financieros y de negocios, lo que lo convierte en un objetivo atractivo para los ciberdelincuentes. Por lo tanto, la evaluación y análisis de vulnerabilidades en los sistemas informáticos del banco es fundamental para detectar debilidades de seguridad y adoptar medidas preventivas y correctivas para proteger los datos de los clientes y los activos de la organización.

Además, el análisis de vulnerabilidades en los servidores del Banco también permitirá identificar y evaluar los riesgos de seguridad asociados con el acceso remoto a los sistemas, la conexión de dispositivos externos y la gestión de datos, entre otros. Por lo tanto, el proyecto contribuirá a mejorar la seguridad de la red y a reducir la probabilidad de sufrir ataques y violaciones de datos.

La justificación del proyecto de análisis de vulnerabilidades en los servidores del Banco es la necesidad de garantizar la seguridad de los datos confidenciales de los clientes y de la organización, y de proteger los activos del banco de los posibles riesgos de seguridad informática. La implementación del proyecto permitirá identificar debilidades de seguridad en los sistemas informáticos del banco y tomar medidas preventivas y correctivas para garantizar la seguridad de la red y reducir la probabilidad de sufrir ataques y violaciones de datos.

Otro factor que justifica la implementación de este proyecto es la creciente regulación en materia de seguridad y privacidad de datos. Los reguladores y organismos gubernamentales de todo el mundo están intensificando sus esfuerzos para garantizar la protección de los datos de los clientes y la privacidad de los usuarios. En muchos países, las empresas están obligadas por ley a adoptar medidas de seguridad específicas para proteger los datos de sus clientes. La implementación del proyecto de análisis de vulnerabilidades en los servidores del Banco permitirá a la organización cumplir con las regulaciones y normativas aplicables en materia de seguridad de datos.

Por último, el proyecto también justifica su implementación debido al rápido avance de la tecnología y las amenazas cibernéticas. Los ciberdelincuentes están constantemente desarrollando nuevas técnicas y herramientas para atacar a las organizaciones y robar información confidencial. Por lo tanto, el análisis de vulnerabilidades en los servidores del Banco debe ser un proceso continuo y actualizado para identificar y mitigar los posibles riesgos de seguridad en tiempo real.

La implementación del proyecto de análisis de vulnerabilidades en los servidores del Banco es esencial para proteger los datos confidenciales de los clientes y los activos de la organización de los posibles riesgos de seguridad informática, cumplir con las regulaciones y normativas aplicables en materia de seguridad de datos y mantenerse actualizado con las amenazas cibernéticas en constante evolución.

DESARROLLO

Metodologías de seguridad:

OCTAVE:

La metodología octave, (Operationally Critical Threat, Asset, and Vulnerability Evaluation por sus siglas en inglés) es una técnica de evaluación de amenazas con el objetivo de implementarse en grandes organizaciones. Esta se compone de tres pasos:

Desarrollar perfiles de Amenaza: En esta fase se identifican los activos o bienes de la empresa vulnerables, así como las practicas que puedan poner en riesgo los mismos.

Identificar vulnerabilidades de infraestructura: En esta fase se analizan cada uno de los elementos de infraestructura y sus respectivas debilidades y/o vulnerabilidades que los vuelven susceptibles ante amenazas externas.

Desarrollar planes y estrategias de seguridad: En esta fase se elaboran estrategias de seguridad y eventuales planes de mitigación teniendo en cuenta los riesgos analizados en el primer y segundo paso.

Se debe destacar que, es una metodología que requiere de amplios conocimientos previos para su implementación, pero, se centra principalmente en la operatividad de la empresa, pasando así la seguridad de la información a un segundo plano. Además, para implementar su uso externo se debe comprar su licencia al SEI (Software Engineering Institute).

MAGERIT:

Magerit es una metodología de análisis y gestión de riesgos de la información desarrollada por el Consejo Superior de Administración Electrónica. Esta metodología tiene como fin estudiar los posibles riesgos a los que se somete un sistema de información, además de recomendar medidas para prevenir, identificar y/o mitigar los riesgos estudiados.

La metodología Margerit, a diferencia de la OCTAVE plantea un análisis más a profundidad de los riesgos de los sistemas de la información, y la importancia de identificarlos a tiempo para crear planes de mitigación, estando relacionado al 100% con el uso de medios electrónicos.

A pesar de esto, la metodología Margerit se considera una metodología costosa al momento de su aplicación, la cual, a pesar de estar enfocada a sistemas de información en el ámbito de la administración, no es recomendable para grandes compañías, precisamente por su tan elevado costo de implementación.

CyberKill Chain:

El CyberKill Chain es entonces una metodología de seguridad que permite identificar y detener los ciberataques de forma temprana, antes de que los mismos puedan causar daños significativos en la infraestructura de una organización. Teniendo en cuenta la carencia de seguridad a nivel de desarrollo de aplicaciones en la empresa, propongo la implementación del CyberKill Chain en la organización, siguiendo los siguientes pasos:

Identificación de la fase de Reconocimiento: En esta fase, se identifican los posibles atacantes y sus tácticas para recopilar información sobre la organización. Se deben realizar análisis periódicos de vulnerabilidades y pruebas de penetración para detectar y corregir posibles puntos débiles en la infraestructura de la organización.

Identificación de la fase de Intrusión: En esta fase, se identifican los posibles ataques a la organización y se toman medidas preventivas para bloquear el acceso no autorizado a la red de la organización. Para ello, se pueden utilizar técnicas de detección de intrusiones, como firewalls y sistemas de detección de intrusiones.

Identificación de la fase de Explotación: En esta fase, se identifican los posibles ataques que pueden explotar vulnerabilidades en el software y hardware de la organización. Se deben implementar medidas de protección, como parches y actualizaciones de software, para corregir posibles vulnerabilidades y prevenir ataques.

Identificación de la fase de Instalación: En esta fase, se identifican los posibles ataques que pueden instalar malware o virus en la red de la organización. Se deben implementar medidas de protección,

como software antivirus y antispyware, para detectar y bloquear la instalación de software malicioso.

Identificación de la fase de Comunicación: En esta fase, se identifican los posibles ataques que pueden comunicar información confidencial de la organización a un tercero no autorizado. Se deben implementar medidas de protección, como sistemas de cifrado y autenticación, para proteger la información confidencial de la organización.

Identificación de la fase de Acción: En esta fase, se identifican los posibles ataques que pueden causar daños en la infraestructura de la organización, como la destrucción de datos o la paralización de los sistemas. Se deben implementar medidas de protección, como sistemas de copia de seguridad y recuperación de desastres, para garantizar la continuidad del negocio en caso de un ataque exitoso.

Figure 1, CyberKill Chain Fuente: https://www.researchgate.net/publication/365820432_Deep_Fake_Detection_Deterrence_and_Response_Challenges_and_Opportunities

METODOLOGIA	VENTAJA	DESVENTAJA
OCTAVE	- Permite su implementación en organizaciones de cualquier tipo. - Perfiles de amenaza basados en los activos de la empresa. - Posee diferentes métodos adaptables a la organización -Relaciona activos con riesgos	- Modelado de amenazas netamente en torno a la funcionalidad de la empresa, no enfocado en los sistemas de información. -Para uso externo se debe pagar su licencia de uso al SEI.
MAGERIT	-Modelado de amenazas complete entorno a los sistemas de información de la empresa. -Sensibiliza sobre la importancia de identificar previamente las amenazas y poder crear planes de mitigación. -Permite que el proceso esté bajo control en todo momento por lo cual es ideal para auditorías y certificaciones.	-A pesar de su uso libre se considera una metodología costosa de aplicar. -Por su elevado costo se recomienda su implementación en organizaciones de trescientos empleados o más.
CYBERKILLCHAIN	-Es una metodología completamente enfocada a la identificación de	-Su implementación puede ser bastante costosa debido a la gran cantidad de recursos,

	vulnerabilidades ante ataques cibernéticos, estando enfocada al cien por ciento para empresas con sistemas de información.	tanto de software, hardware, y humanos para ejercer un control continuo.

Table 1, Comparativa entre distintas metodologías de seguridad

PROPUESTA DE POSIBLE IMPLEMENTACION

Podemos afirmar entonces después de analizar las distintas ventajas y desventajas que ofrece cada una de estas metodologías, y teniendo en cuenta el entorno en donde se llevaría a cabo una posible implementación (Entidad Financiera), que la implementación del modelo CyberKill Chain sería la más adecuada, ya que esta tiene un enfoque enteramente centrado en la detección de vulnerabilidades en sistemas de información. La implementación de este modelo en la empresa permitiría mejorar la seguridad en el desarrollo de aplicaciones, al establecer un proceso sistemático y estructurado de identificación y prevención de posibles ataques. La metodología permitiría identificar posibles vulnerabilidades y amenazas a nivel de desarrollo, antes de que las aplicaciones sean lanzadas a producción, lo que garantizaría el cumplimiento de los requerimientos de seguridad necesarios antes de su lanzamiento.

Por otro lado, el desarrollo del proyecto de análisis de vulnerabilidades en los servidores del Banco se llevará a cabo en varias fases para garantizar una evaluación completa y exhaustiva de la seguridad de los sistemas informáticos del banco. A continuación, se describe cada fase del proyecto en detalle:

Planificación y alcance del proyecto: En esta fase, se definirán los objetivos del proyecto, se establecerá el alcance de la evaluación de vulnerabilidades y se asignarán los recursos necesarios para llevar a cabo el proyecto. Se establecerá un equipo de trabajo con expertos en ciberseguridad y se definirán los plazos y el presupuesto del proyecto.

Identificación de activos y sistemas críticos: En esta fase, se identificarán los activos y sistemas críticos del Banco, como servidores, bases de datos y aplicaciones web, que contienen información confidencial y son esenciales para el funcionamiento de la organización.

Análisis de vulnerabilidades y evaluación de riesgos: En esta fase, se llevará a cabo una evaluación de vulnerabilidades y riesgos en los sistemas y aplicaciones identificadas en la fase anterior. Se utilizarán herramientas de escaneo de vulnerabilidades y se llevarán a cabo pruebas de penetración para identificar debilidades en la seguridad de los sistemas y aplicaciones.

Análisis de políticas de seguridad y controles: En esta fase, se analizarán las políticas de seguridad y los controles existentes del Banco, como firewalls, antivirus, sistemas de detección de intrusos, entre otros. Se evaluará la efectividad de estas políticas y controles para detectar y prevenir ataques cibernéticos y se propondrán mejoras necesarias para fortalecer la seguridad de los sistemas.

Documentación de resultados y propuestas de mejora: En esta fase, se documentarán los resultados de la evaluación de vulnerabilidades y riesgos, y se elaborará un informe detallado que incluya las debilidades identificadas y las propuestas de mejora. Se presentará un plan de acción concreto que detalle las mejoras que deben realizarse en los sistemas y aplicaciones para fortalecer la seguridad de la organización.

Implementación de mejoras: En esta fase, se implementarán las mejoras propuestas en la fase anterior para fortalecer la seguridad de los sistemas y aplicaciones del Banco. Se realizarán pruebas de seguridad posteriores a la implementación para verificar la efectividad de las mejoras realizadas.

Monitoreo y mantenimiento continuo: En esta fase, se establecerá un programa de monitoreo y mantenimiento continuo de los sistemas y aplicaciones del Banco para detectar y mitigar nuevas vulnerabilidades de seguridad en tiempo real. Se recomienda llevar a cabo evaluaciones de vulnerabilidades periódicas para garantizar que los sistemas del banco permanezcan seguros y actualizados.

En conclusión, el proyecto de análisis de vulnerabilidades en los servidores del Banco es esencial para identificar y mitigar los posibles riesgos de seguridad informática y garantizar la protección de los datos confidenciales de los clientes y los activos de la organización. El proyecto se llevará a cabo en varias fases, desde la planificación y alcance hasta el monitoreo y mantenimiento continuo, para garantizar una evaluación completa y exhaustiva de la seguridad de los sistemas

IDENTIFICACIÓN Y ANÁLISIS DE VULNERABILIDADES PARA EL BANCO MEDIANTE PRUEBAS DE PENETRACIÓN

Una de las soluciones más efectivas para identificar y analizar las vulnerabilidades en los sistemas de seguridad del Banco es la realización de pruebas de penetración o "Pentesting". El Pentesting es una técnica que consiste en simular un ataque informático sobre los sistemas del banco para evaluar su resistencia y detectar las debilidades en su seguridad. De esta manera, se puede conocer el nivel de seguridad de los sistemas y tomar medidas para mejorarlos.

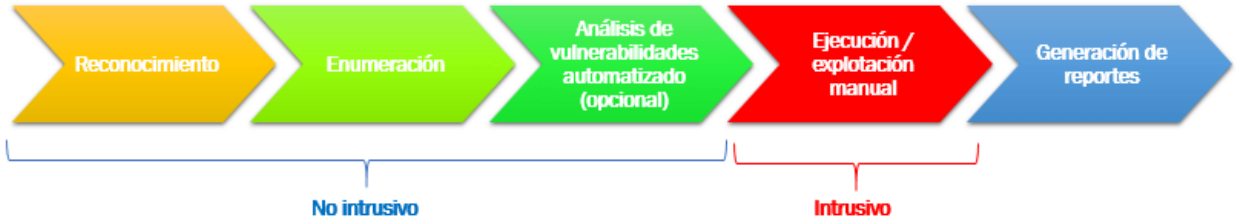

Figure 2, Diagrama de fases de un Pentesting. Fuente: https://www.ma-no.org/es/seguridad/introduccion-al-pentesting

Para llevar a cabo una prueba de penetración efectiva, se debe seguir un proceso sistemático que cubra todos los aspectos relevantes de los sistemas a evaluar. A continuación, se presentan las fases típicas de un proyecto de Pentesting:

1. **Recopilación de información:** se recopila información relevante sobre el objetivo del Pentesting, incluyendo direcciones IP, nombres de dominio, servicios y aplicaciones que se ejecutan en los servidores del Banco.

Para llevar a cabo esta fase, se pueden utilizar diferentes técnicas y herramientas de análisis de red, como el escaneo de puertos, el descubrimiento de servidores y servicios, la identificación de sistemas operativos y la recolección de información sobre los nombres de dominio y las direcciones IP asociadas a los servidores del Banco.

Una de las herramientas más comunes para la recolección de información es el escaneo de puertos, que permite identificar los servicios que están ejecutándose en un servidor determinado. Por ejemplo, se pueden utilizar herramientas como Nmap para realizar un escaneo de puertos en los

servidores del Banco y obtener información sobre los servicios que están disponibles en cada uno de ellos.

Otra técnica común para la recolección de información es el "banner grabbing", que implica la obtención de información sobre los servicios de red a partir de la respuesta que estos proporcionan al establecer una conexión. Por ejemplo, se puede utilizar la herramienta Netcat para conectarse a un servicio determinado y obtener información sobre la versión del software que está siendo utilizado.

En el caso del Banco, la recolección de información debería realizarse de forma cuidadosa y con el consentimiento de la entidad financiera. Es importante asegurarse de que se está trabajando en un entorno controlado y no se está afectando el funcionamiento normal de los sistemas.

Una vez que se ha recopilado la información necesaria, se debe realizar un análisis detallado de la misma, con el fin de identificar posibles vulnerabilidades y puntos débiles en los sistemas del Banco. En esta etapa, se pueden utilizar herramientas de análisis de vulnerabilidades, como Nessus o OpenVAS, para escanear los sistemas en busca de posibles vulnerabilidades.

2. **Análisis de vulnerabilidades:** se realizan pruebas automatizadas y manuales para detectar las vulnerabilidades de seguridad en los sistemas. Esto incluye la evaluación de la configuración de los firewalls, la revisión de los parches y actualizaciones de seguridad, y la búsqueda de vulnerabilidades conocidas en el software y las aplicaciones.

En el caso del Banco, en esta fase se realizaría un análisis detallado de los resultados obtenidos en la fase de recolección de información, para identificar los posibles puntos de entrada de los atacantes y las vulnerabilidades en los sistemas y aplicaciones. Se llevarían a cabo pruebas de penetración para evaluar la resistencia del sistema a los ataques y simular situaciones de riesgo.

Las técnicas de escaneo se utilizan para identificar los sistemas y aplicaciones en el alcance del proyecto, incluyendo sistemas operativos, servidores web, bases de datos y otros componentes del

sistema. Se pueden utilizar herramientas automatizadas para realizar escaneos de puertos y servicios, y para identificar las versiones de software y los parches de seguridad disponibles.

Una vez identificados los sistemas y aplicaciones en el alcance del proyecto, se pueden realizar pruebas de exploración para identificar las vulnerabilidades de seguridad. Esto implica utilizar técnicas de prueba y error para encontrar posibles debilidades en la configuración del sistema, como contraseñas débiles o vulnerabilidades en el software.

En el caso del Banco, se pueden utilizar herramientas especializadas para realizar pruebas de penetración y evaluar la resistencia del sistema a los ataques. Estas pruebas pueden incluir el intento de acceder a sistemas y aplicaciones sin autorización, la identificación de vulnerabilidades en la configuración del firewall y otros componentes del sistema, y la explotación de vulnerabilidades conocidas en el software.

Es importante destacar que esta fase debe ser realizada por expertos en seguridad informática con conocimientos técnicos avanzados, ya que las pruebas pueden involucrar el uso de herramientas y técnicas sofisticadas que requieren un alto nivel de experiencia.

3. **Explotación de vulnerabilidades:** Una vez identificadas las vulnerabilidades, se simulan ataques para evaluar la efectividad de las medidas de seguridad existentes y la capacidad de los sistemas para resistir los ataques. En esta fase, se intenta explotar las debilidades de los sistemas para obtener acceso no autorizado a los servidores o comprometer la información confidencial.

   En el caso del Banco, la fase de Explotación de Vulnerabilidades implicaría realizar pruebas para verificar si es posible explotar las vulnerabilidades identificadas en la fase anterior. Esto podría incluir intentar obtener acceso no autorizado a los sistemas mediante técnicas de hacking o ingeniería social, o intentar ejecutar comandos maliciosos para obtener información o tomar control del sistema.

   Para llevar a cabo esta fase, se podría utilizar una combinación de herramientas de hacking y técnicas de ingeniería social, en función de las vulnerabilidades específicas

identificadas en la fase anterior. Algunas de las herramientas que podrían utilizarse incluyen Metasploit, Nmap, Nessus, y herramientas de escaneo de puertos.

Es importante tener en cuenta que esta fase debe ser llevada a cabo con extremo cuidado y sólo por personal capacitado en técnicas de hacking ético.

Además, debe contar con la autorización y el consentimiento previo del Banco, y debe llevarse a cabo en un entorno controlado y aislado de la red de producción del banco para evitar daños a los sistemas y la exposición de datos confidenciales.

Una vez que se han realizado las pruebas de explotación de vulnerabilidades, el Pentester deberá documentar los resultados y las recomendaciones para mitigar las vulnerabilidades identificadas. Con base en los resultados obtenidos en esta fase, se podrán identificar medidas adicionales para mejorar la seguridad de los sistemas y minimizar los riesgos de seguridad informática.

4. **Informe de resultados:** Se elabora un informe detallado que incluya los resultados del Pentesting, las vulnerabilidades identificadas, el grado de riesgo asociado a cada vulnerabilidad, las recomendaciones para mitigar los riesgos y mejorar la seguridad del sistema.

   El informe de resultados debe proporcionar una visión general de los resultados generales del pentesting y una evaluación de la eficacia de los controles de seguridad actuales del Banco. Esto puede ayudar a la dirección del banco a tomar decisiones informadas sobre las inversiones en seguridad y a mejorar su postura general de seguridad.

   Para la realización de la fase de informe de resultados en el caso del Banco, se recomienda utilizar un formato de informe claro y conciso, que presente los hallazgos de manera clara y fácil de entender para los miembros del equipo de seguridad y la dirección del banco. Además, se recomienda incluir recomendaciones específicas para corregir las vulnerabilidades encontradas y sugerir un plan de acción claro y factible

para mitigar los riesgos. También es importante proporcionar una visión general de los resultados generales y las áreas de mejora, para ayudar al banco a mejorar su postura de seguridad en general.

5. **Seguimiento y verificación:** una vez implementadas las medidas de seguridad recomendadas, se verifica su efectividad mediante la realización de pruebas de penetración adicionales para comprobar que las vulnerabilidades han sido mitigadas.

   En el caso del Banco, se debe llevar a cabo una evaluación periódica para asegurarse de que las medidas de mitigación implementadas son efectivas y detectar posibles nuevas vulnerabilidades. También se debe actualizar y mejorar continuamente las medidas de seguridad para garantizar la protección continua de la empresa, para ello se puede seguir el siguiente procedimiento:

   1. Realizar un seguimiento de las vulnerabilidades: es importante mantener un registro de las vulnerabilidades identificadas durante el pentesting. Se debe actualizar este registro con la información de las medidas de mitigación implementadas y la fecha de su implementación.

   2. Verificar la efectividad de las medidas de mitigación: se debe realizar una verificación para asegurarse de que las medidas de mitigación implementadas son efectivas. Esto implica realizar pruebas para asegurarse de que las vulnerabilidades han sido eliminadas o reducidas a un nivel aceptable.

   3. Realizar pruebas de penetración periódicas: se recomienda realizar pruebas de penetración periódicas para asegurarse de que las medidas de mitigación siguen siendo efectivas y para detectar nuevas vulnerabilidades que puedan surgir.

   4. Actualizar y mejorar continuamente las medidas de seguridad: es importante estar actualizado con las últimas amenazas de seguridad y tecnologías de mitigación. Por lo tanto, se debe realizar una evaluación continua de las medidas de seguridad y actualizarlas regularmente para garantizar la protección continua de la empresa.

CONCLUSIONES

- Es necesaria la implementación de un programa de monitoreo y mantenimiento continuo de los sistemas de información de la entidad financiera, con el fin de detectar y mitigar nuevas vulnerabilidades y así mantener seguros los mismos.

- La implementación del Modelo de Cyberkill Chain puede mejorar en un gran porcentaje la seguridad de una empresa en el ámbito de TI. En el caso de la entidad financiera, al establecer un proceso sistemático y estructurado para identificar y prevenir posibles ataques se estaría protegiendo de manera más efectiva la información.

- Las pruebas de penetración "Pentesting" son una solución efectiva para identificar y analizar las vulnerabilidades en los sistemas de información de la entidad financiera. Esto siguiendo la metodología del CyberKill Chain.

- Se debe realizar un continuo seguimiento de las vulnerabilidades identificadas y verificar la efectividad de las medidas de mitigación implementadas. Es recomendable realizar pruebas de penetración periódicas para así ver la resistencia de los sistemas ante estas amenazas, y actualizar continuamente las medidas de seguridad para mantener la protección de los sistemas de la empresa.

BIBLIOGRAFIA

Liu, Y., & Chen, M. (2019). Cybersecurity of Financial Institutions: An Analysis of Threats and Solutions. Journal of Risk and Financial Management, 12(3), 120.

Scarfone, K., & Mell, P. (2011). Guide to Intrusion Detection and Prevention Systems (IDPS). National Institute of Standards and Technology.

Aleem, S., Khan, F. A., & Vasilakos, A. V. (2019). A Comprehensive Review of Cybersecurity Threats, Vulnerabilities, and Current Defensive Measures. IEEE Access, 7, 122042-122060.

Liao, Z., & Liu, Y. (2019). Cybersecurity Risk Assessment for Financial Institutions Based on the Analytic Hierarchy Process. Journal of Risk Research, 22(4), 462-477.

Sookhak, M., Alazab, M., & Khan, M. K. (2019). A Comprehensive Survey of Security Issues in Internet of Things. Journal of Network and Computer Applications, 126, 11-34.

Veltsistas, P. G., Tsalgatidou, A., & Gritzalis, S. (2019). Enhancing the Security of Cloud-based Banking Applications. Journal of Information Security and Applications, 48, 102377.

Vista de Pentesting empleando técnicas de Ethical Hacking en redes IPv6. (s/f). Edu.co. Recuperado de https://revistas.ufps.edu.co/index.php/ingenio/article/view/2096/2044

López Jaramillo, D. M., & Vásquez Mejía, S. A. (2016). Comparación entre metodologías de gestión de riesgo informático. Universidad del Azuay.

Vista de Metodologías para el análisis de riesgos en los sgsi. (s/f). Edu.co. Recuperado de https://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874

Jiménez, M., & Noheli, J. (2021). Mapeo sistemático de metodologías de Seguridad de la Información para el control de la gestión de riesgos informáticos.

Molina, L., & del Pilar, A. (2019). Pentesting Web. https://repository.unad.edu.co/handle/10596/25188

Cruz, H., & Liliana, M. (2018). Gestión de riesgo, metodologías Octave y Magerit. Universidad Piloto de Colombia.