TAREA 3 – MODELADO DE AMENAZAS

JHON SEBASTIAN ZUÑIGA LOPEZ

TUTOR SERGIO LUIS LUDO ARGUMEDO

GRUPO 55

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERIA
INGENIERIA EN SISTEMAS
Argelia – Cauca
febrero 2022

Objetivo

Evaluar riesgos de seguridad de la información en los procesos de desarrollo de software utilización de plataformas de terceros, en línea con los estándares y políticas de seguridad establecidos por la organización.

Diseñar simulación de varios servicios en red por medio del software análisis y modelado tool 2016.

Documentar las amenazas obtenidas del escaneo de vulnerabilidades echo al diseño establecido para la realización de pruebas

Presentación en línea

Link:
https://www.canva.com/design/DAGC60IocZ4/nMJSeMQab7AWOa7VO4GTNg/edit?utm_content=DAGC60IocZ4&utm_campaign=designshare&utm_medium=link2&utm_source=sharebutton

Diagrama de flujos de datos (DFD)

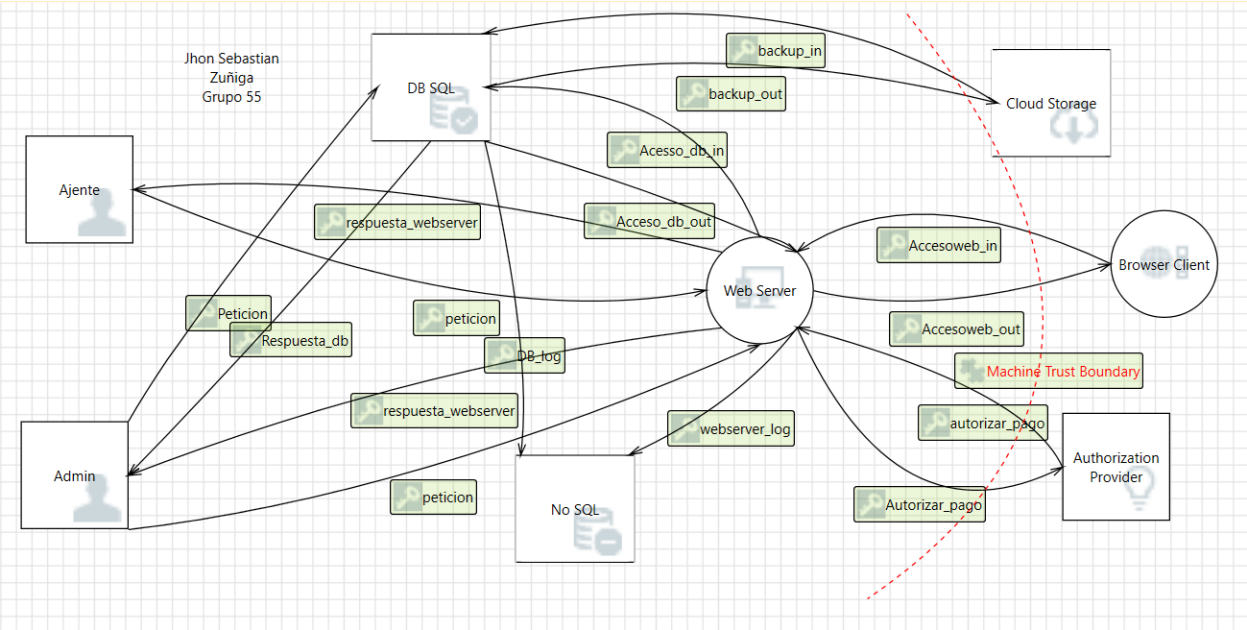

Table 1. Documentación de amenazas

Descripción de la amenaza	Objetivo	Técnicas de ataque
Falsificación de la entidad externa Agente	Un atacante puede falsificar Agente y esto puede dar lugar a un acceso no autorizado al servidor web. Considere utilizar un mecanismo de autenticación estándar para identificar la entidad externa.	Suplantación de identidad
Almacén de datos inaccesible	Un agente externo impide el acceso a un almacén de datos al otro lado del límite de confianza	Denegación de servicios

Elevación cambiando el flujo de ejecución en el servidor web	Un atacante puede pasar datos al servidor web para cambiar el flujo de ejecución del programa dentro del servidor web según su elección.	Elevación de privilegios
Agente de entidad externa potencialmente niega haber recibido datos	Agente afirma que no recibió datos de un proceso al otro lado del límite de confianza. Considere utilizar el registro o la auditoría para registrar la fuente, la hora y el resumen de los datos recibidos.	repudio
El servidor web puede estar sujeto a elevación de privilegios mediante la ejecución remota de código	El Agente puede ejecutar código de forma remota para el servidor web.	Elevación de privilegios

Tabla 2. Calcular riesgos

	Probabilidad de ocurrencia(P)			**Potencia del impacto(I)**		**P**	**I**	**Riesgo**
Amenaza	***R***	***E***	***DI***	***D***	***A***	***(R+E+DI)***	***(D+A)***	***PxI***
Falsificación de la entidad externa Agente	3	2	3	3	3	8	6	48
Almacén de datos inaccesible	3	3	3	3	2	9	5	45
Elevación cambiando el flujo de ejecución en el servidor web	2	3	2	2	3	7	5	35
Agente de entidad externa potencialmente niega haber recibido datos	1	3	2	3	2	6	5	30

El servidor web puede estar sujeto a elevación de privilegios mediante la ejecución remota de código	2	2	2	1	3	6	4	24

Tabla 3. Salvaguardas

descripción de la amenaza	Un atacante puede falsificar Agente y esto puede dar lugar a un acceso no autorizado al servidor web. Considere utilizar un mecanismo de autenticación estándar para identificar la entidad externa.
Medidas de seguridad	1. Mecanismo de autenticación estándar. 2. Doble verificación. 3. Realizar pruebas de penetración. 4. Crear el acceso basado en roles.
Descripción de la amenaza	Un agente externo impide el acceso a un almacén de datos al otro lado del límite de confianza
Medidas de seguridad	1. Realizar autenticaciones solidas. 2. Encriptar los datos en tráfico y en reposo 3. Hacer uso de un firewall
Descripción de la amenaza	Un atacante puede pasar datos al servidor web para cambiar el flujo de ejecución del programa dentro del servidor web según su elección.
Medidas de seguridad	1. Validar todas las entradas de datos 2. Tener todos los sistemas actualizados 3. Gestionar las autenticaciones 4. Dar privilegios mínimos al servidor
Descripción de la amenaza	Agente afirma que no recibió datos de un proceso al otro lado del límite de confianza. Considere utilizar el registro o la auditoría para registrar la fuente, la hora y el resumen de los datos recibidos.
Medidas de seguridad	1. Cifrar todo dato que este en tráfico. 2. Realizar registros junco con auditorias. 3. Monitorear en cada momento la red.

	4. Realizar autenticaciones y control de acceso robusto
descripción de la amenaza	El Agente puede ejecutar código de forma remota para el servidor web.
Medidas de seguridad	1. Realizar filtrado de la red por medio de firewalls 2. Realizar actualizaciones regulares. 3. Limitar los privilegios en el servidor

Referencias bibliográficas

Chris Bronk. (2016). Cyber Threat: The Rise of Information Geopolitics in U.S. National Security. Praeger. https://bibliotecavirtual.unad.edu.co/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=1140402&lang=es&site=eds-live&scope=site&ebv=EB&ppid=pp_41

Death, D. (2017). Information Security Risk Management. En S. Editing (Eds), Information Security Handbook (p.p 66 – 83). Packt Publishing. https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=1655557&lang=es&site=eds-live&scope=site&ebv=EB&ppid=pp_183

https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=602994&lang=es&site=eds-live&scope=site&ebv=EB&ppid=pp_101

Marmolejo, P.A. (2021). Principios de la seguridad de la información y Propiedades del Software seguro. https://repository.unad.edu.co/handle/10596/41638

Ramachandran, M. (2012). Design for software security. En Nova (Eds), Software Security Engineering : Design and Applications (pp. 101-112). Nova Science Publishers, Inc.