Vulnerabilidades de Sistemas Operativos

Integrantes:

- Ernesto Santiago, Caycho Cuellar

- Juan Dominid, Muñoz Eslava

- Jefferson Andy Gomez Calderon

1. INICIO DEL PROYECTO
   1. Acta de Constitución del Proyecto

Nombre del proyecto: Vulnerabilidades de Sistemas Operativos

Objetivos generales

* Concienciar sobre la importancia del conocimiento en sistemas operativos como base para la ciberseguridad, destacando su papel en la identificación, prevención y mitigación de vulnerabilidades.
* Analizar vulnerabilidades reales como BlueKeep y EternalBlue para comprender su impacto y la necesidad de una gestión proactiva de la seguridad.
* Promover buenas prácticas de seguridad tanto para administradores de sistemas como para desarrolladores, con un enfoque en la prevención de amenazas y la protección de datos.
* Fomentar la implementación de medidas técnicas y organizativas efectivas, tales como actualizaciones de software, configuración de firewalls y respaldo de información, como parte de una estrategia integral de defensa

Patrocinador o líder del proyecto

Lider: JUAN DOMINID MUÑOZ ESLAVA

Stakeholders clave (interesados)

Presupuesto

* 1. Identificación de stakeholders

Lista de interesados del proyecto

1. PLANIFICACIÒN DEL PROYECTO
   1. Definición del alcance del proyecto

Se describe que es lo incluye y lo que no incluye

Este proyecto tiene como alcance el análisis y la exposición de la importancia del conocimiento en sistemas operativos y su relación directa con la seguridad informática. Se enfoca en:

* Examinar vulnerabilidades críticas que han afectado ampliamente a sistemas operativos, como BlueKeep y EternalBlue.
* Describir los riesgos asociados tanto a nivel organizacional como individual debido a la explotación de dichas vulnerabilidades.
* Proponer medidas técnicas y de gestión que fortalezcan la postura de seguridad, incluyendo configuraciones específicas, actualizaciones, controles de acceso y monitoreo.
* Brindar buenas prácticas orientadas a administradores de sistemas y desarrolladores para prevenir, detectar y responder ante amenazas de seguridad.
  1. Cronograma de proyecto

Se define por semanas de trabajo.

Se listan todas las actividades a realizarse hasta terminar la implementación

* 1. Costos del proyecto
  2. Plan de recursos humanos

JEFFERSON ANDY GOMEZ CALDERON

JUAN DOMINID MUÑOZ ESLAVA

ERNESTO SANTIAGO CAYCHO CUELLAR

* 1. Gestión de riesgos
  2. Riesgos para Organizaciones

Impacto Financiero:

* Pérdidas económicas por interrupción de servicios
* Costos de recuperación y remediación
* Multas regulatorias por incumplimiento
* Daño a la reputación corporativa

Impacto Operacional:

* Interrupción de servicios críticos
* Pérdida de datos sensibles
* Compromiso de sistemas de infraestructura
* Tiempo de inactividad prolongado
  1. Riesgos para Usuarios

Impacto Financiero:

* Robo de información personal y financiera
* Acceso no autorizado a sistemas personales
* Instalación de malware y spyware
* Pérdida de privacidad

Impacto Operacional:

* Exposición de datos regulados (GDPR, HIPAA, etc.)
* Responsabilidad legal por negligencia
* Pérdida de confianza de clientes y socios

1. IMPLEMENTACIÒN DEL PROYECTO

Se debe mostrar la simulación del proyecto y los resultados del  
mismo

1. PASE A OPERACIÒN Y CIERRE DEL PROYECTO

✓ Pase a operación de evidencia con un correo formal al área de operaciones de la empresa,

indicando los resultados del proyecto y el estado en que se deja la red.

✓ El cierro del proyecto es el resumen de resultados de este con las conclusiones de los resultados.