Benyahir Y. Martínez Hermina R00624824

Asignación 1 – Fundamentos de la Ciberseguridad y Vulnerabilidades:

Caso de uso – Red de la Compañía CyberCorp (12pts)

#	Activo / Ubicación	Vulnerabilidad	Categoría	Impacto CIA	Escala CVSS	Recomendación
1	Servidor de Escritorio Remoto, puerto **3389/TCP**	**CVE-2019-0708**	Humano	C – El atacante puede robar los datos personales de los usuarios que estén adentro del servidor. I – El atacante puede permitir que aplicaciones maliciosas se instalen en el sistema. A – El servidor puede estar fuera de servicio por un periodo no determinado de tiempo.	10.0	Remediar

#	Activo / Ubicación	Vulnerabilidad	Categoría	Impacto CIA	Escala CVSS	Recomendación
2	Print Spooler, Servidor de archivos y el controlador de dominio	**CVE-2021-34527**	Lógica	C – El atacante puede tener acceso a archivos importantes adentro del servidor I – Este puede manipular distintos aspectos en los archivos adentro del servidor. A – Riesgo de los archivos que presente el servidor no sean los correctos.	9.0	Mitigar

Preguntas Teóricas (8pts)

1. ¿Qué es la seguridad cibernética y cuáles son sus componentes principales (Tríada CIA)? Incluye 1 ejemplo práctico de C, I y A.

   Es una metodología que permite la protección de equipos, sistemas importantes y datos de atacantes digitales. Sus componentes principales son la confidencialidad, integridad y disponibilidad. La confidencialidad se encarga que los datos adentro de un servidor no sean visibles de una manera pública, en la integridad se encarga de asegurar que los datos adentro no se puedan modificar, mantenerlos de una manera segura y la disponibilidad es lo que permite que los datos adentro del servidor sean accesible cuando estos sean necesario.

2. Diferencia entre vulnerabilidad, amenaza y riesgo. Proporciona un ejemplo breve que las conecte.

   Una vulnerabilidad se podría ver como una apertura en un sistema que si no se remedia o mitiga pude ser explotada. Mayormente es por parte de una amenaza/atacante que al encontrar la vulnerabilidad para hacer con ella lo que sea y con ello tenemos que medir el riesgo que nos dicta cuanto el impacto que la amenaza tendrá.

3. CVSS v3.1: ¿qué miden AV, AC, PR, UI y cómo influyen en el resultado base? Indica los rangos Bajo/Medio/Alto/Crítico.

   AV – mide si la vulnerabilidad puede ser explotada de una manera remota o por una conexión en la internet.
   AC – mide la complejidad del ataque si este es alto o bajo.
   PR – mide los privilegios que el atacante requiere.
   UI – mide si el usuario requiere hacer alguna interacción para que la vulnerabilidad sea explotada.

   Estas métricas influyen gravemente a la hora de medir la escala de CVSS donde si la gran mayoría de las métricas son cumplidas de manera que el atacante explote una vulnerabilidad esto designaría que ese ataque sea tenga una escala de 9.0 – 10 (Crítico), si el ataque fuese de una menos leve pero aun hace pasa por casi todas las métricas la escala seria 7.0 – 8.9 (Alto), si los ataques son de menor intensidad caerían en la escala con la calificación de 4.0 – 6.9 (Medio) y de aun menor de intensidad esto caen en la escala con 0.0 – 3.9 (Bajo).

4. Tratamiento del riesgo: diferencia remediar, mitigar, aceptar; da un ejemplo realista de cada uno.

   Digamos que un atacante entro a un servidor de una manera donde este entro directamente sin la necesidad de alguna credencial y en el proceso modifico varios archivos, para este tipo de riesgo lo más razonable es remediar donde se tiene que corregir por completo la vulnerabilidad de ese servidor de acceso libre. En otro servidor se encuentra periódicamente siendo atacado por parte de atacantes que entran a este con credenciales oficiales de la compañía / negocio, la mejor manera de lidiar con esto mitigar donde reducimos las probabilidades de que estos entren a atacar el servidor aumentando la seguridad de este con MFA. Como ultimo caso tenemos un servidor donde los ataques hacia este son casi nunca y si ocurren el servidor están fuertemente protegidos para impedirlos, el tratamiento que este requerirse es aceptar ya que los riesgos que aparecen en este servidor son tan bajos no se necesitan hacer ninguna rutina de tratamiento.

5. Elige uno de tus dos hallazgos. Supón que parchear tarda 10 días. Escribe mínimo 3 oraciones explicando:

   - 2–3 acciones sencillas que aplicarías mientras llega el parche (cosas que puedes hacer tú mismo en el equipo/servicio).

   - Cómo esas acciones mantienen la Disponibilidad y ayudan a proteger la Confidencialidad e Integridad (Tríada CIA).

   - Qué riesgo residual quedaría aún con esas acciones temporales.

   Hallazgo elegido: 2021 – Print Nightmare – 34527

   La primera acción que aplicaría seria sacar y bloquear el servicio al servidor del atacante. Como segunda acción me enfocaría en inspeccionar los datos adentro del servidor para anotar y notificar los cambios que los atacantes modificaron en el sistema a los encargados del parche. Finalmente notificaría a los empleados de la compañía que tuvieran acceso al servidor que cambien sus credenciales para entrar a este debido a que el atacante usaba sus credenciales para acceder a este.