**Trabajo Practico**

Materia: Auditoria y Seguridad Informatica

Alumno: Vietto Santiago

Profesor: Alfredo Luis Pardo

Intitucion: UCC

Año: 2021

**1)\_ Politicas de cuentas**

1.1)\_ Politicas de contraseñas (Password Policy)

**1.1.1\_** (L1 - automated) Ensure 'Enforce password history' is set to '24 or more password(s)': asegurar de que “exigir el historial de contraseñas” esté configurado en 24 o más contraseñas.

Descripcion: esta configuración determina la cantidad de contraseñas únicas renovadas que deben asociarse con una cuenta de usuario antes de poder reutilizar una contraseña anterior. Donde el estado recomendado para esta configuración es de 24 o más contraseñas.

Valor por defecto: 0

Consideraciones: cuanto más tiempo un usuario utilice la misma contraseña, mayor será la posibilidad de que un atacante pueda determinar la contraseña mediante ataques de fuerza bruta. Además, cualquier cuenta que pueda haber sido comprometida seguirá siendo explotable mientras no se modifique la contraseña. Por eso si se especifica un número bajo para esta configuración, los usuarios podrán usar el mismo número reducido de contraseñas de forma repetida, ademas los usuarios pueden cambiar repetidamente sus contraseñas hasta que puedan reutilizar su contraseña original.

**1.1.2\_** (L1 - automated) Ensure 'Maximum password age' is set to '60 or fewer days, but not 0': asegurar de que la “Antigüedad máxima de la contraseña” esté establecida en 60 días o menos, pero no en 0.

Descripcion: esta configuración define cuánto tiempo un usuario puede usar su contraseña antes de que caduque. Los valores oscilan entre 0 y 999 días. Si establece el valor en 0, la contraseña nunca caducará. Ya a que los atacantes pueden descifrar contraseñas, cuanto mas frecuente se cambie la contraseña, menos chances tendrá un atacante de desifrar la contraseña y utilizarla. Sin embargo, cuanto más bajo se establezca este valor, mayor será la posibilidad de que aumenten las llamadas al servicio de asistencia técnica debido a que los usuarios tengan que cambiar su contraseña o se olviden de la contraseña actual. El estado recomendado para esta configuración es 60 días o menos, pero no 0.

Valor por defecto: 42 dias

Consideraciones: cuanto más tiempo exista una contraseña, mayor será la probabilidad de que se vea comprometida por un ataque de fuerza bruta, por un atacante que obtenga conocimientos generales sobre el usuario o por el usuario que comparte la contraseña. Tener esta configuracion en 0 para que el usuarios nunca tenga que cambiar sus contraseñas, es un riesgo de seguridad importante porque permite que el usuario malintencionado utilice una contraseña comprometida mientras el usuario válido tenga acceso autorizado.

**1.1.3\_** (L1 - automated) Ensure 'Minimum password age' is set to '1 or more day(s)': asegurar de que la “antigüedad mínima de la contraseña” esté establecida en 1 día o más.

Descripcion: esta configuración determina la cantidad de días que debe usar una contraseña antes de poder cambiarla. El rango de valores para esta configuración de directiva es de entre 1 y 999 días. (También puede establecer el valor en 0 para permitir cambios de contraseña inmediatos). El estado recomendado para esta configuración es: 1 o más días.

Valor por defecto: 0

Consideraciones: como los usuarios suelen tener contraseñas favoritas que se usan porque son fáciles de recordar y a veces se piensa que esa contraseña está a salvo de compromisos, pero por mala suerte, las contraseñas están comprometidas y si un atacante tiene como objetivo la cuenta de usuario de un individuo específico, con conocimiento previo de los datos sobre ese usuario, la reutilización de contraseñas antiguas puede causar una brecha de seguridad. Esta configuración evita la fácil reutilización de contraseñas antiguas. Es por eso que se debe configurar en un número mayor que 0 para que la configuración “Enforce password history” sea efectiva.

**1.1.4\_** (L1 - automated) Ensure 'Minimum password length' is set to '14 or more character(s)': asegurar de que la “longitud mínima de la contraseña” esté establecida en 14 o más caracteres.

Descripcion: esta configuración determina la menor cantidad de caracteres que componen una contraseña para una cuenta de usuario. Los usuarios deben estar informados sobre esta selección y del mantenimiento adecuado de las contraseñas, especialmente con respecto a la longitud de las mismas. En entornos empresariales, el valor ideal para esta configuración es de 14 caracteres; sin embargo, debe ajustar este valor para cumplir con los requisitos comerciales de su organización. Por ende el estado recomendado para esta configuración es 14 o más caracteres.

Valor por defecto: 0

Consideraciones: los tipos de ataques de contraseña incluyen ataques de diccionario (que intentan usar palabras y frases comunes) y ataques de fuerza bruta (que prueban todas las combinaciones posibles de caracteres). Además, los atacantes a veces intentan obtener la base de datos de la cuenta para poder usar herramientas para descubrir las cuentas y contraseñas.

**1.1.5\_** (L1 - automated) Ensure 'Password must meet complexity requirements' is set to 'Enabled': asegurar de que “La clave debe cumplir los requerimientos de complejidad” esté configurada como enable (habilitada).

Descripcion: esta configuración verifica todas las contraseñas nuevas para asegurarse de que cumplan con los requisitos básicos de contraseñas seguras. Cuando esta política está habilitada, las contraseñas deben cumplir los siguientes requisitos mínimos:

* No contener el nombre de la cuenta del usuario o partes del nombre completo del usuario que excedan dos caracteres consecutivos
* Tener al menos seis caracteres de longitud.
* Contener personajes de tres de las siguientes categorías:
* Caracteres en mayúsculas en inglés (de la A a la Z)
* Caracteres en minúscula en inglés (de la a a la z)
* Base de 10 dígitos (0 a 9)
* Caracteres no alfabéticos (por ejemplo,!, $, #,%)
* Una categoría general de cualquier carácter Unicode que no se encuentre en las cuatro categorías anteriores. Esta quinta categoría puede ser regionalmente específica.

Cada carácter adicional en una contraseña aumenta su complejidad de manera exponencial.

Valor por defecto: disable

Consideraciones: las contraseñas que contienen solo caracteres alfanuméricos son extremadamente fáciles de descubrir con varias herramientas disponibles públicamente.

**1.1.7\_** (L1 - automated) Ensure 'Store passwords using reversible encryption' is set to 'Disabled': asegurar de que “Almacenar contraseñas mediante cifrado reversible” esté configurado como disable (deshabilitado).

Descripcion: esta configuración determina si el sistema operativo almacena las contraseñas de una manera que utiliza cifrado reversible, que proporciona compatibilidad con los protocolos de aplicación que requieren el conocimiento de la contraseña del usuario para fines de autenticación. Las contraseñas que se almacenan con cifrado reversible son esencialmente las mismas que las versiones de texto sin formato de las contraseñas. El estado recomendado para esta configuración es: Desactivado.

Valor por defecto: disable

Consideraciones: habilitar esta configuración permite que el sistema operativo almacene contraseñas en un formato más débil que es mucho más susceptible de comprometerse y debilita la seguridad de su sistema.

1.2)\_ Política de bloqueo de cuenta (Account Lockout Policy)

**1.2.1\_** (L1 - automated) Ensure 'Account lockout duration' is set to '15 or more minute(s)': asegurar de que la “Duración del bloqueo de la cuenta” esté configurada en 15 o más minutos.

Descripcion: esta configuración determina el período de tiempo que debe transcurrir antes de que se desbloquee una cuenta bloqueada y asi el usuario pueda intentar iniciar sesión de nuevo. La configuración no estará disponible. Si el valor de esta configuración de directiva se configura en 0, las cuentas bloqueadas permanecerán bloqueadas hasta que un administrador las desbloquee manualmente. El estado recomendado para esta configuración es 15 o más minutos.

Valor por defecto: no tiene ninguno, porque esta configuración de política solo tiene significado cuando se especifica un umbral de bloqueo de la cuenta. Cuando se configura un umbral de bloqueo de la cuenta, Windows sugiere automáticamente un valor de 30 minutos.

Consideraciones: Se puede crear una condición de denegación de servicio (DoS) si un atacante abusa del umbral de bloqueo de la cuenta e intenta repetidamente iniciar sesión con una cuenta específica. Una vez que configure el umbral de bloqueo de la cuenta, la cuenta se bloqueará después del número especificado de intentos fallidos. Si configura la opción Duración del bloqueo de la cuenta en 0, la cuenta permanecerá bloqueada hasta que un administrador la desbloquee manualmente.

**1.2.2\_** (L1 - automated) Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0': asegurar de que el “Umbral de bloqueo de cuenta” esté configurado en 10 o menos intentos de inicio de sesión no válidos, pero no 0.

Descripcion: esta configuración determina el número de intentos fallidos de inicio de sesión antes de que se bloquee la cuenta. Establecer esta en 0 no se ajusta al punto de referencia, ya que al hacerlo, se inhabilita el umbral de bloqueo de la cuenta. Entonces el estado recomendado para esta configuración es 10 o menos intentos de inicio de sesión no válidos, pero no 0.

Valor por defecto: 0

Consideraciones: establecer un umbral de bloqueo de cuenta reduce la probabilidad de que un ataque de fuerza bruta de contraseña en línea tenga éxito. Establecer este umbral de bloqueo demasiado bajo presenta el riesgo de un aumento de los bloqueos accidentales y/o un actor malintencionado puede que bloquee intencionalmente las cuentas.

**1.2.3\_** (L1 - automated) Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)': asegurar de que “Restablecer contador de bloqueo de cuenta después de” esté configurado en 15 o más minutos.

Descripcion: esta configuración determina el período de tiempo antes de que el umbral de bloqueo de la cuenta se restablezca a cero. El valor predeterminado para esta configuración es deshabilitado. Si se define el umbral de bloqueo de la cuenta, este tiempo de restablecimiento debe ser menor o igual que el valor de la configuración de duración del bloqueo de la cuenta.

Si deja esta configuración de directiva en su valor predeterminado o configura el valor en un intervalo demasiado largo, su entorno podría ser vulnerable a un ataque DoS (denegacion de servicio). Donde un atacante podría realizar de forma maliciosa varios intentos fallidos de inicio de sesión en todos los usuarios de la organización, lo que bloqueará sus cuentas. El estado recomendado para esta configuración es: 15 o más minutos.

Valor por defecto: no tiene ninguno, porque esta configuración de política solo tiene significado cuando se especifica un umbral de bloqueo de la cuenta. Cuando se configura un umbral de bloqueo de la cuenta, Windows sugiere automáticamente un valor de 30 minutos.

Consideraciones: los usuarios pueden bloquear accidentalmente sus cuentas si escriben mal su contraseña varias veces. Para reducir la posibilidad de tales bloqueos accidentales, el contador Restablecer bloqueo de cuenta después de la configuración, determina la cantidad de minutos que deben transcurrir antes de que el contador que rastrea los intentos fallidos de inicio de sesión y desencadena bloqueos se restablezca a 0.