Ejercicio Práctico: Seguridad de Sistema y Control de Acceso en Windows 10/11

Objetivo del Ejercicio

Aprender a restringir el acceso a una aplicación y a aplicar una política de seguridad que refuerce las contraseñas, utilizando el **Firewall de Windows** y las **Políticas de Seguridad Local (secpol.msc)**.

Escenario

La empresa "SecureNet" tiene las siguientes necesidades de seguridad:

1. **Seguridad de Red (Firewall):** Necesitan bloquear temporalmente el uso de la aplicación de correo electrónico **Outlook** para **tráfico saliente** (evitar envío de información) y **tráfico entrante** (evitar recepción de correos) como medida de contingencia.
2. **Seguridad Local (Políticas):** Necesitan asegurar que todos los usuarios locales utilicen contraseñas fuertes que contengan al menos **12 caracteres**.

Instrucciones Paso a Paso: Parte 1 - Configuración del Firewall

Tarea 1.1: Bloquear el Tráfico Saliente (Regla de Salida)

1. **Abrir el Firewall de Windows con Seguridad Avanzada:**
   - Pulsa la tecla de **Windows + R** para abrir el diálogo "Ejecutar".
   - Escribe `wf.msc` y presiona **Enter**. (Esto abre la consola del Firewall avanzado).
2. **Crear la Regla de Salida:**
   - En el panel izquierdo, selecciona **"Reglas de salida"**.
   - En el panel derecho, haz clic en **"Nueva regla..."**.
3. **Configurar el Asistente:**
   - **Tipo de regla:** Selecciona **"Programa"** → **"Siguiente"**.

- **Programa:** Haz clic en **"Examinar..."** y navega a la ubicación del ejecutable de Outlook. La ruta típica es: `C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE` (o la ruta correspondiente a la versión instalada) → **"Siguiente"**.
- **Acción:** Selecciona **"Bloquear la conexión"** → **"Siguiente"**.
- **Perfiles:** Asegúrate de que los tres perfiles (**Dominio, Privado, Público**) estén marcados → **"Siguiente"**.
- **Nombre:** Dale un nombre descriptivo, por ejemplo: `BLOCK_OUT_Outlook_Salida` → **"Finalizar"**.

Tarea 1.2: Bloquear el Tráfico Entrante (Regla de Entrada)

1. **Crear la Regla de Entrada:**
   - En el panel izquierdo, selecciona **"Reglas de entrada"**.
   - En el panel derecho, haz clic en **"Nueva regla..."**.
2. **Configurar el Asistente:**
   - **Tipo de regla:** Selecciona **"Programa"** → **"Siguiente"**.
   - **Programa:** Usa la misma ruta del ejecutable de Outlook que en el paso anterior → **"Siguiente"**.
   - **Acción:** Selecciona **"Bloquear la conexión"** → **"Siguiente"**.
   - **Perfiles:** Asegúrate de que los tres perfiles estén marcados → **"Siguiente"**.
   - **Nombre:** Dale un nombre descriptivo, por ejemplo: `BLOCK_IN_Outlook_Entrada` → **"Finalizar"**.

Tarea 1.3: Comprobación y Reversión

1. **Comprobación (Opcional):** Intenta abrir Outlook y enviar/recibir un correo. Debería fallar o mostrar errores de conexión.
2. **Reversión:** Para que Outlook vuelva a funcionar, selecciona las dos reglas creadas (`BLOCK_OUT_Outlook_Salida` y `BLOCK_IN_Outlook_Entrada`) y haz clic derecho → **"Deshabilitar regla"** o **"Eliminar"**.

Instrucciones Paso a Paso: Parte 2 - Políticas de Seguridad Local (secpol.msc)

Tarea 2.1: Reforzar la Política de Contraseñas (Mínimo de 12 Caracteres)

1. **Abrir la Consola de Políticas de Seguridad Local:**
   - Pulsa la tecla de **Windows + R**.
   - Escribe `secpol.msc` y presiona **Enter**. (Esto abre el Editor de Políticas de Seguridad Local).
2. **Navegar a la Configuración de Contraseñas:**
   - En el panel izquierdo, navega a **"Directivas de cuentas" → "Directiva de contraseñas"**.
3. **Modificar la Longitud Mínima de la Contraseña:**
   - Haz doble clic en la directiva **"Longitud mínima de la contraseña"**.
   - En la ventana de propiedades, cambia el valor a **12** → **"Aplicar" → "Aceptar"**.
   - *(Nota: El valor predeterminado en muchas instalaciones es 0 o 7).*
4. **Verificar Otras Configuraciones (Opcional pero Relacionado):**
   - Verifica que la directiva **"La contraseña debe cumplir los requisitos de complejidad"** esté habilitada (suele ser el valor predeterminado).

Tarea 2.2: Aplicar y Comprobar la Política

1. **Forzar la Actualización de Políticas (Recomendado):**
   - Abre el **Símbolo del sistema** o **PowerShell** como **Administrador**.
   - Ejecuta el comando: `gpupdate /force`
   - Esto asegura que las políticas locales se apliquen inmediatamente.
2. **Comprobación:**
   - Vuelve al **Administrador de Equipos** (como en el ejercicio anterior) → **"Usuarios y Grupos Locales" → "Usuarios"**.
   - Intenta crear un nuevo usuario con una contraseña corta (por ejemplo, `123456`).
   - **Resultado Esperado:** Windows debe mostrar un mensaje de error indicando: *"No se puede actualizar la contraseña. El valor proporcionado para la nueva contraseña no cumple con los requisitos de longitud, complejidad o historial de dominio."*
3. **Reversión (Volver al estado anterior):**
   - Vuelve a **secpol.msc → "Directiva de contraseñas"**.

- Cambia el valor de **"Longitud mínima de la contraseña"** a 7 (o el valor inicial si lo anotaste) → **"Aplicar"** → **"Aceptar".**

Puntos a Discutir

- **Alcance del Firewall:** ¿Por qué es necesario crear **dos reglas** (entrada y salida) para bloquear completamente una aplicación? (Respuesta: El tráfico debe bloquearse en ambas direcciones para garantizar el aislamiento total de la red).
- **Prioridad y Perfiles:** ¿Qué significan los perfiles de red (**Dominio, Privado, Público**) y cómo influyen en la aplicación de la regla del Firewall? (Respuesta: Permiten aplicar reglas solo cuando la red es confiable/privada o cuando están en una red pública/no segura).
- **Alcance de secpol.msc**: Las políticas de secpol.msc solo se aplican a los **usuarios locales** de esa máquina. ¿Qué herramienta se usaría en un entorno de red grande (Active Directory) para aplicar estas políticas a miles de usuarios a la vez? (Respuesta: **Directiva de Grupo** (gpedit.msc o la Consola de Administración de Directivas de Grupo en el servidor)).
- **Seguridad Obligatoria:** ¿Por qué la política de contraseñas es una forma de control de acceso más fuerte que simplemente pedir a los usuarios que usen contraseñas largas? (Respuesta: Obliga al sistema a cumplir el requisito, el usuario no tiene elección).