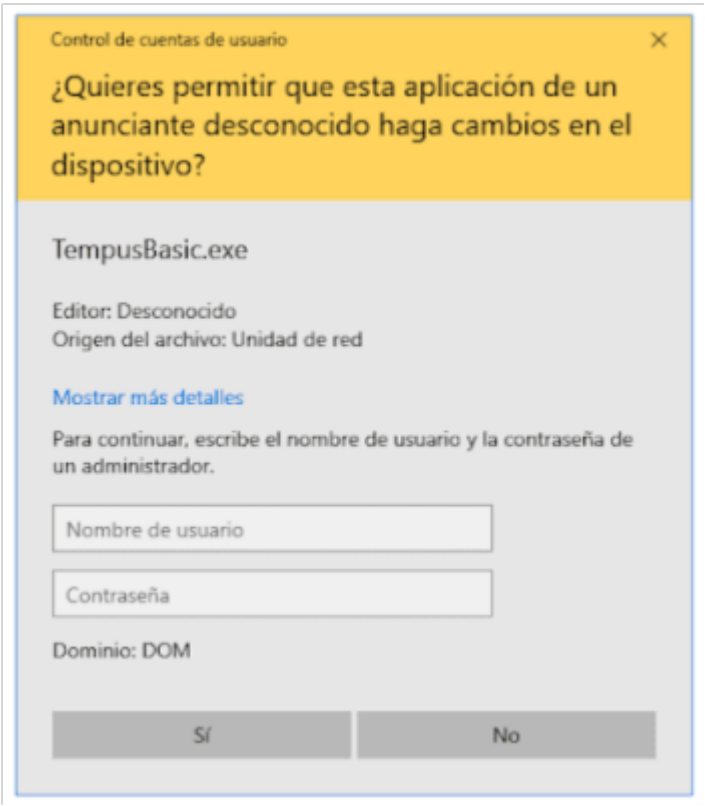
Microsoft Windows: Ejecutar un programa usando RUNAS.

En el laboratorio de hoy vamos a ver, como podemos ejecutar un programa que requiere permisos administrativos que la cuenta de usuario de un equipo cliente no posee, usando el comando llamado **RUNAS**.
Además, también podremos ver los inconvenientes que supone usar el comando **RUNAS**.

Cuando hablamos de las buenas practicas, en los equipos conectados a un entorno de dominio de ***Active Directory***. Posiblemente la primera de ellas es, que los usuarios no tengan permisos de administrador local en sus equipos.

Pero si restringimos los permisos de los usuarios en sus propios equipos, puede suceder que un programa requiera esos permisos para su ejecución y nos solicite las credenciales de ***Administrador*** del dominio para poder ser ejecutado.



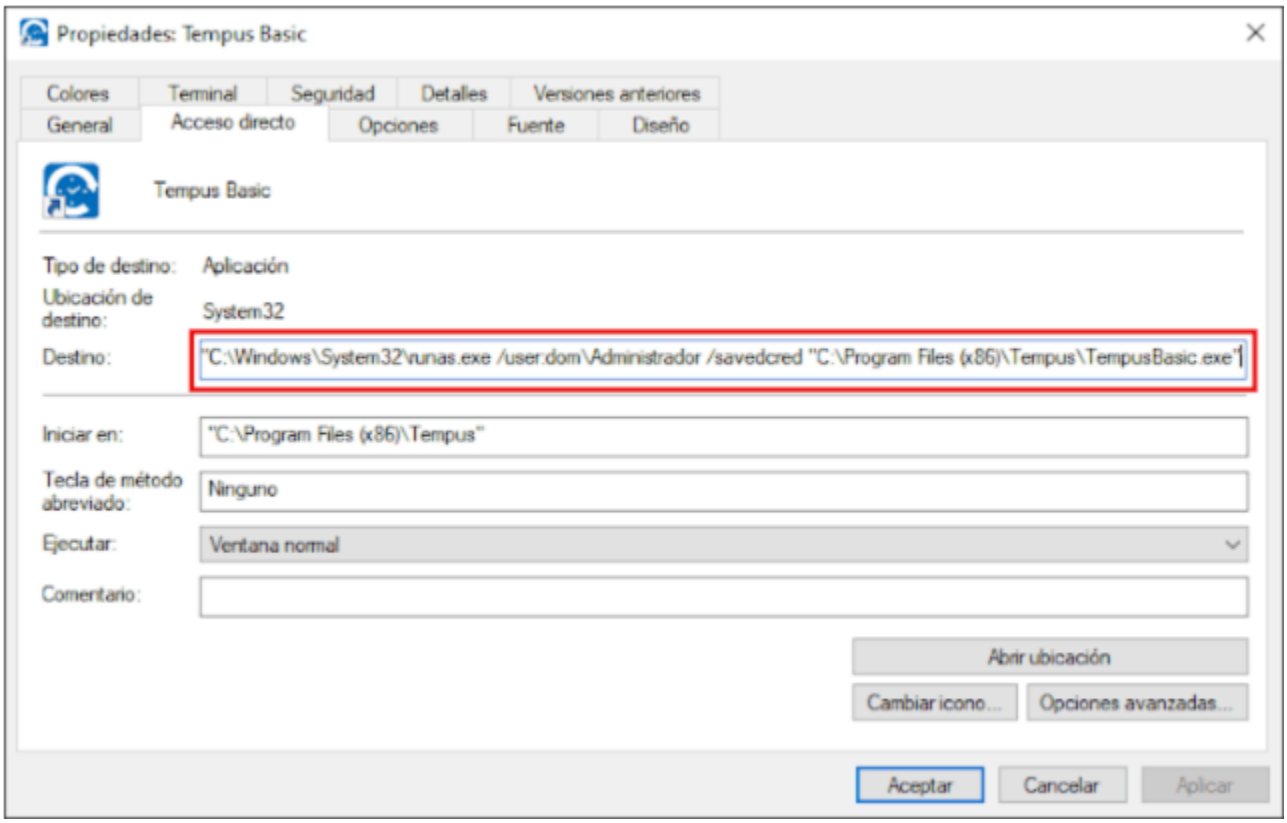
Una solución que aplican muchos administradores de red es, ejecutar el programa conflictivo usando el comando llamado **RUNAS**.

El procedimiento es sumamente sencillo. En primer lugar, editaríamos el acceso directo del programa que requiere permisos ampliados para ser ejecutado, y cambiaríamos el destino del acceso directo por la construcción que mostramos a continuación:

```
C:\Windows\System32\runas.exe /user:dominio\nombre_usuario /savedcred
"ruta_programa_conflictivo\nombre_ejecutable"
```

La construcción final para nuestro laboratorio será la siguiente.

```
C:\Windows\System32\runas.exe /user:dom\Administrador /savedcred "C:\Program
Files (x86)\Tempus\TempusBasic.exe"
```



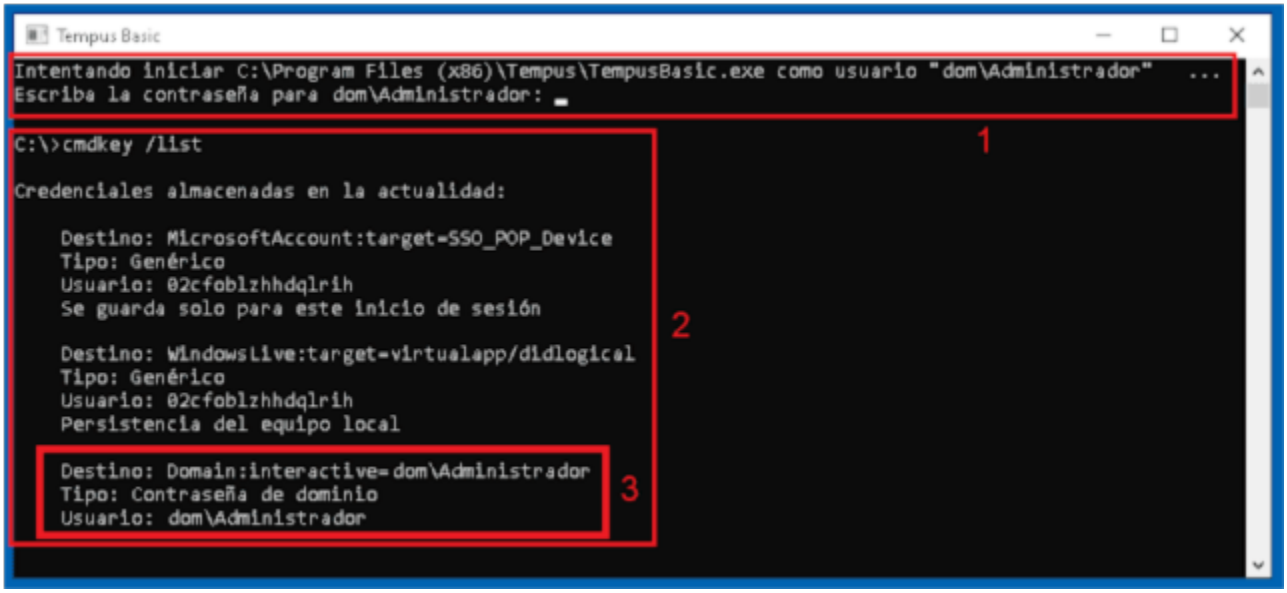
Una vez realizados los cambios, deberemos ejecutar desde la cuenta de ***Administrador*** el acceso directo modificado del programa. Esta ejecución, nos solicitará la contraseña de ***Administrador*** de dominio, una vez la hayamos introducido, esta será almacenada en nuestro equipo.

```
Intentando iniciar C:\Program Files (x86)\Tempus\TempusBasic.exe como usuario
"dom\Administrador" ...
Escriba la contraseña para dom\Administrador:
```

Usando el comando llamado **`cmdkey /list`**, podemos comprobar que que la contraseña de administrador del dominio realmente ha sido almacenada en nuestro equipo local.

```
cmdkey /list

Credenciales almacenadas en la actualidad:

    Destino: MicrosoftAccount:target=SSO_POP_Device
    Tipo: Genérico
    Usuario: 02cfoblzhhdqlrih
    Se guarda solo para este inicio de sesión

    Destino: WindowsLive:target=virtualapp/didlogical
    Tipo: Genérico
    Usuario: 02cfoblzhhdqlrih
    Persistencia del equipo local

    Destino: Domain:interactive=dom\Administrador
    Tipo: Contraseña de dominio
    Usuario: dom\Administrador
```

A partir de este momento, cuando el usuario ejecute el acceso directo modificado del programa, este será ejecutado usando las credenciales de ***Administrador*** almacenadas en nuestro equipo.



Una vez que ya sabemos como ejecutar un programa con permisos de ***Administrador*** haciendo uso del comando **RUNAS**, vamos a ver la parte negativa de esta práctica tan extendida.

Analicemos que hace **RUNAS**.

Si ejecutamos **RUNAS** sin el modificador **/savedcred**, podemos comprobar que la ejecución nos solicitará directamente la contraseña del usuario ***Administrador***. Una vez hayamos introducido la contraseña se intentará iniciar el programa, si la contraseña es correcta el programa será iniciado.

Usando el comando llamado **cmdkey /list** podemos comprobar que la contraseña del usuario Administrador no ha sido almacenada en nuestro equipo porque no hemos incluido el modificador **/savedcred**

```
runas.exe /user:dom\Administrador "C:\Program Files (x86)\Tempus\TempusBasic.exe"
Escriba la contraseña para dom\Administrador:
Intentando iniciar C:\Program Files (x86)\Tempus\TempusBasic.exe como usuario
"dom\Administrador" ...
```

A continuación, realizaremos misma ejecución de **RUNAS** agregando el modificador **/savedcred**. En primer lugar comprobaremos, que la ejecución intentará buscar las credenciales de ***Administrador*** almacenadas en nuestro equipo, si no las encuentra, nos solicitará la contraseña del usuario ***Administrador***. Una vez hayamos introducido la contraseña se intentará iniciar el programa, una segunda vez, usando la contraseña introducida. Si la contraseña es correcta, el programa será iniciado y la contraseña será almacenada en nuestro equipo local para poder ser usada en futuras ejecuciones.

```
runas.exe /user:dom\Administrador /savedcred "C:\Program Files (x86)
\Tempus\TempusBasic.exe"
Intentando iniciar C:\Program Files (x86)\Tempus\TempusBasic.exe como usuario
"dom\Administrador" ...
Escriba la contraseña para dom\Administrador:
Intentando iniciar C:\Program Files (x86)\Tempus\TempusBasic.exe como usuario
"dom\Administrador" ...
```

Usando el comando llamado **cmdkey /list** podemos comprobar que que la contraseña de administrador de nuestro dominio de Active Directory, realmente ha sido almacenada en nuestro equipo local.

```
cmdkey /list

Credenciales almacenadas en la actualidad:

    Destino: WindowsLive:target=virtualapp/didlogical
    Tipo: Genérico
    Usuario: 02cfoblzhhdqlrih
```

```
Persistencia del equipo local

Destino: Domain:interactive=dom\Administrador
Tipo: Contraseña de dominio
Usuario: dom\Administrador
```

A partir de este momento, cuando el usuario ejecute el acceso directo modificado del programa este será ejecutado con las credenciales de ***Administrador***.

```
runas.exe /user:dom\Administrador /savedcred "C:\Program Files (x86)
\Tempus\TempusBasic.exe"
Intentando iniciar C:\Program Files (x86)\Tempus\TempusBasic.exe como usuario
"dom\Administrador" ...
```

¿Que problema tiene el uso de esta práctica?

Si almacenamos las credenciales del usuario ***Administrador*** en nuestros equipos cliente, cualquier persona que use la construcción **`runas.exe /user:dom\Administrador /savedcred`** podrá ejecutar cualquier programa que desee usando las credenciales del usuario ***Administrador*** de nuestro dominio de Active Directory sin necesidad de saber la contraseña con anterioridad. Eso supone un grandísimo agujero de seguridad en nuestra red.

En nuestro próximo laboratorio vamos ver como eliminar las contraseñas almacenadas en nuestros equipos cliente.

Espero os sea de utilidad.