UAC Bypass – Task Scheduler

pentestlab.blog/category/red-team/page/118

May 3, 2017

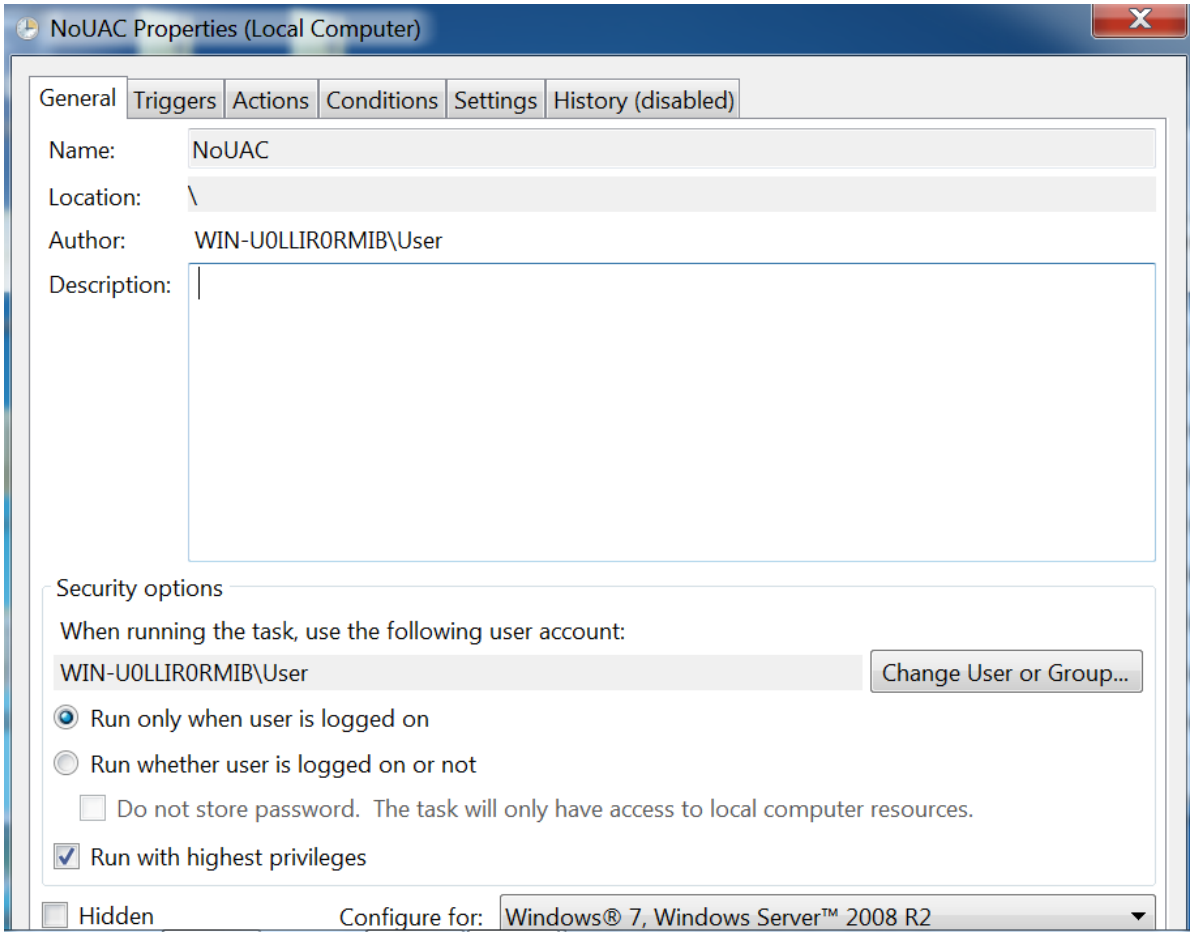
Windows Task Scheduler can be abused in order to bypass User Account Control (UAC) if the user has access to its graphical interface. This is due to the fact that the security option run with highest privileges when the user is creating a new task doesn't require from the user to authenticate with an administrator account.

The method below can be used in situations where there is a direct access to the system either via RDP or physical.

Creation of a new schedule task can be done either from command line or from the Task Scheduler interface.

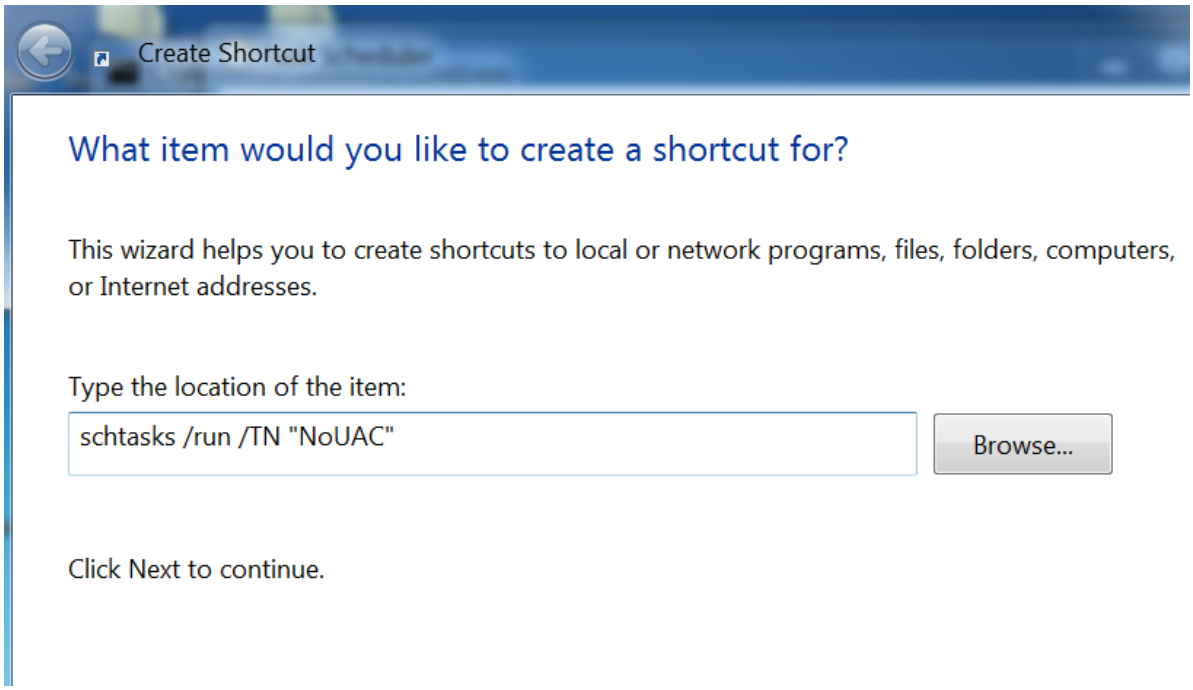
```
C:\>SchTasks /Create /SC DAILY /TN "NoUAC" /TR "C:\Users\User\Desktop\pentestlab3
.exe" /ST 23:36
```

From the properties of the task in task scheduler interface the option **"Run with highest privileges"** must be checked.



Task Scheduler – High Privilege Option

A windows shortcut can be created as a quick method to launch the task without having to open task scheduler or to wait for the task to be executed at the specific time.

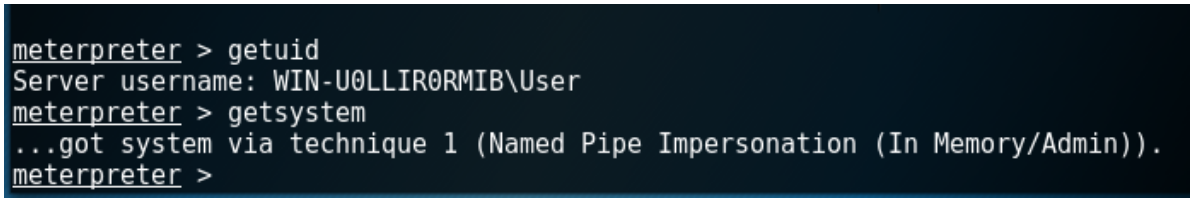


Windows Shortcut – Schedule Task

In the location of the item field the following command should be inserted:

```
schtasks /run /TN "NoUAC"
```

Since the task will be executed with the highest privileges the UAC will not request for elevation.



Task Scheduler – Elevated Meterpreter