

Windows Privilege Escalation: Insecure GUI Application

October 14, 2021 By Raj Chandel

Introduction

In the series of Privilege escalation, till now we have learned that Microsoft Windows offers a wide range of fine-grained permissions and privileges for controlling access to Windows components including services, files, and registry entries. Today through applications we are going to exploit the privileges. Many GUI applications need higher privileges other than the current user to have, to access some of their particular services. Secondly, just due to misconfiguration of the application. Let's deep dive into it.

Table of Content

- Introduction
- Prerequisites
- Lab setup of insecure GUI Application
- Abusing Insecure GUI Application

Prerequisites:

Machine A-Windows 10 (Ignite as an admin user)

Notepad++ Installed application on Windows 10


Lab Setup of Insecure GUI Application


Machine A, has ignite as an admin user.

Now, by the `whoami /priv` command, we get to know that "Ignite" an admin user has only 5 privileges of shut down, change notification etc. with the enable and disable state which is displayed in the below screenshot

```
whoami /priv
```

We have to understand that if any user has admin access even though that user does not have full or higher privileges.

```
C:\Users\ignite>whoami /priv 
PRIVILEGES INFORMATION
-----
Privilege Name      Description              State
-----
SeShutdownPrivilege Shut down the system     Disabled
SeChangeNotifyPrivilege Bypass traverse checking Enabled
SeUndockPrivilege   Remove computer from docking station Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled
SeTimeZonePrivilege Change the time zone     Disabled

C:\Users\ignite>net user demo /add 
System error 5 has occurred.

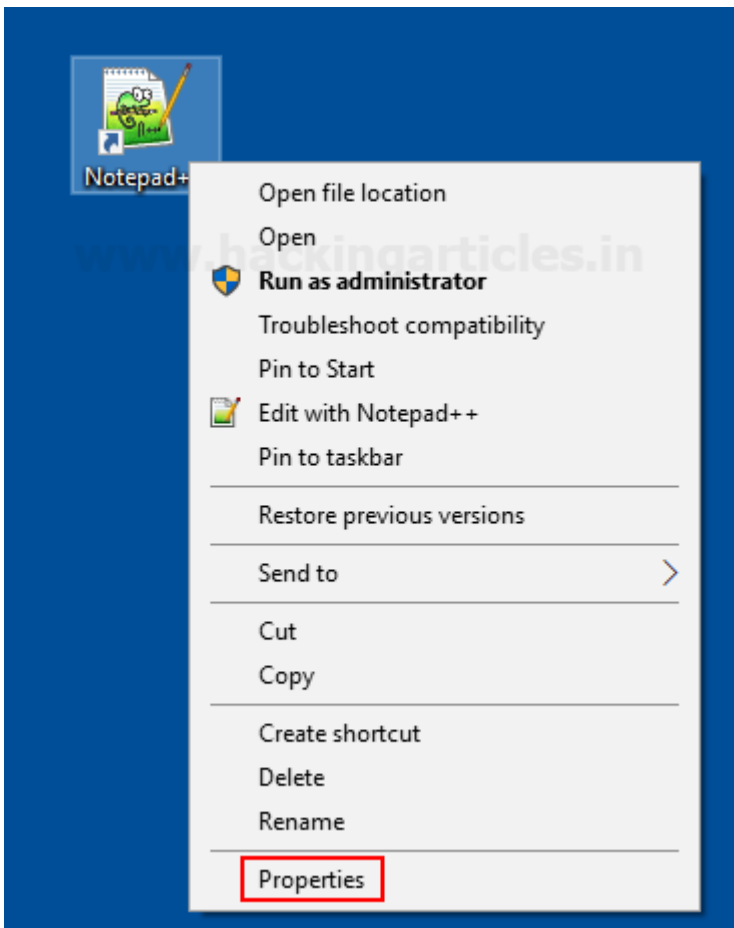
Access is denied.

C:\Users\ignite>_
```

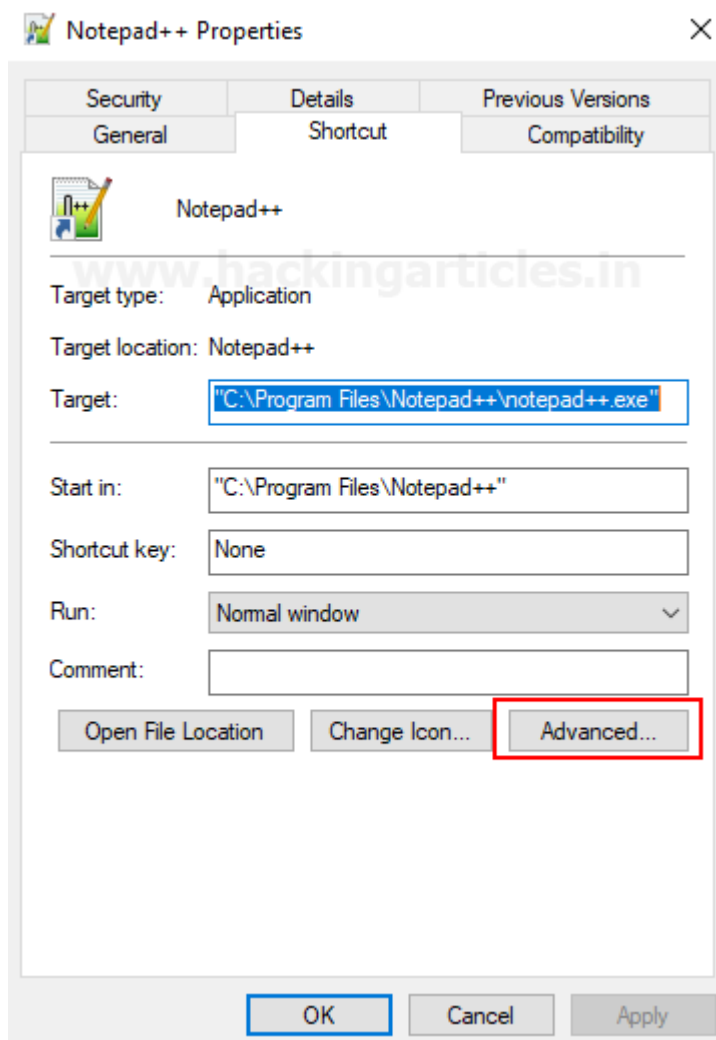
Now we will check the ignite admin user's privileges by adding a new user "demo". Unfortunately, access is denied. It means "ignite" user does not have full higher privileges.

Install Notepad++ on window 10 and misconfigure the application or insecure it by providing the run as administrator.

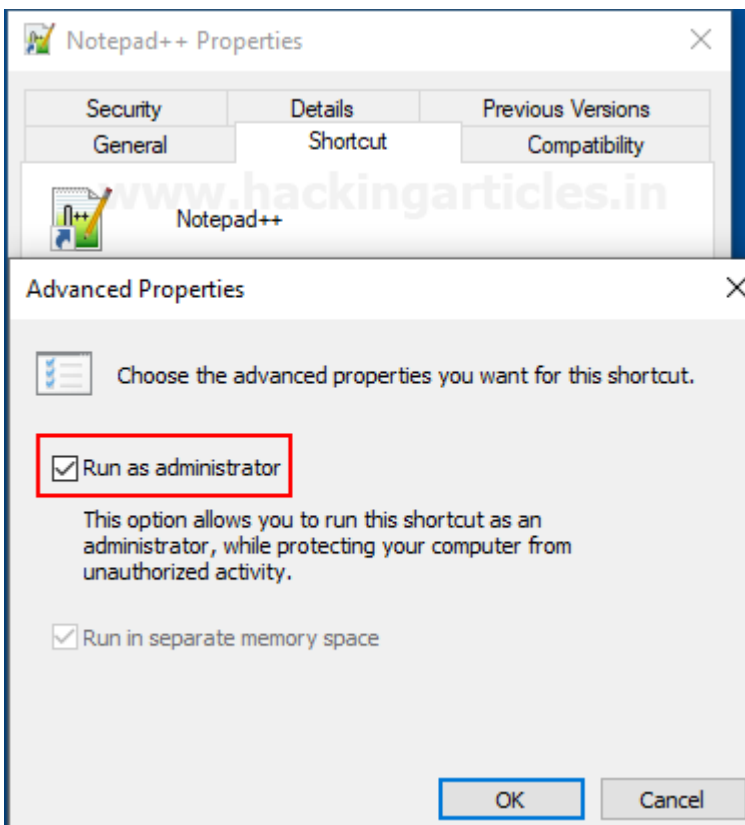
Right-click on the **Notepad++** icon and click on the properties to edit **advance** settings.



Edit the Notepad++ properties just by click on advanced and then ok, by default it will display some of the information of Notepad++ properties as mentioned in the following screenshot.



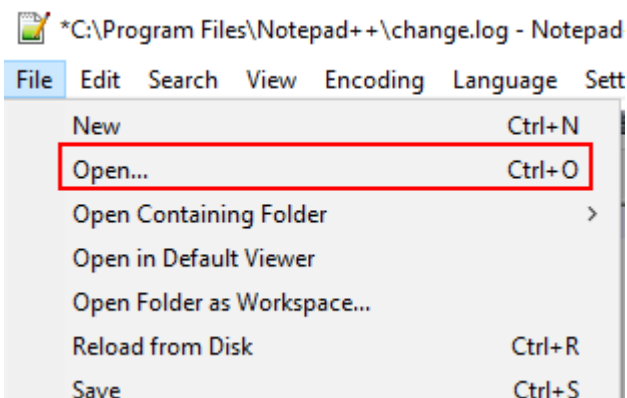
In the next window of advanced properties, there is an option to run the application as an administrator. Just tick the option and click on OK. Now whenever we will execute the Notepad++ automatically it will run as administrator.



Abusing Insecure GUI Application

After enumerate some time on windows applications, we found that the Notepad++ application has a feature that allows us to open the file, the short key to open the file is CTRL+O or by navigating to the option File then go to open.

Note: In lab set up we had already granted permission to run as administrator, whenever we execute the Notepad++.



The next open prompt will allow us to run a binary with the same privilege escalation same as the Notepad++ process.

Just by entering the cmd exe in the navigating bar, it will open a command prompt.

Now, the Command prompt will open with the Notepad++'s administrator privileges. The following command will display all the privileges names, descriptions and enabled and disabled features

If it will allow operations like to open a command prompt or to run executable with the high privileges then it will allow escalating the privileges.

This demonstrates that admin user “ignite” does not have the same privileges as the Notepad++ application that runs as an administrator. Just compare the first and last screenshots for a better understanding. We will characterize this as privilege escalation even though we can now add any new user through the command line. Finally, demo user is successfully added and take the advantage of insecure GUI application to exploit the privileges.

```
C:\Program Files\Notepad++>whoami /priv
```

PRIVILEGES INFORMATION

Privilege Name	Description
SeIncreaseQuotaPrivilege	Adjust memory quotas for a process
SeSecurityPrivilege	Manage auditing and security log
SeTakeOwnershipPrivilege	Take ownership of files or other objects
SeLoadDriverPrivilege	Load and unload device drivers
SeSystemProfilePrivilege	Profile system performance
SeSystemtimePrivilege	Change the system time
SeProfileSingleProcessPrivilege	Profile single process
SeIncreaseBasePriorityPrivilege	Increase scheduling priority
SeCreatePagefilePrivilege	Create a pagefile
SeBackupPrivilege	Back up files and directories
SeRestorePrivilege	Restore files and directories
SeShutdownPrivilege	Shut down the system
SeDebugPrivilege	Debug programs
SeSystemEnvironmentPrivilege	Modify firmware environment values
SeChangeNotifyPrivilege	Bypass traverse checking
SeRemoteShutdownPrivilege	Force shutdown from a remote system
SeUndockPrivilege	Remove computer from docking station
SeManageVolumePrivilege	Perform volume maintenance tasks
SeImpersonatePrivilege	Impersonate a client after authentication
SeCreateGlobalPrivilege	Create global objects
SeIncreaseWorkingSetPrivilege	Increase a process working set
SeTimeZonePrivilege	Change the time zone
SeCreateSymbolicLinkPrivilege	Create symbolic links
SeDelegateSessionUserImpersonatePrivilege	Obtain an impersonation token for a session user

```
C:\Program Files\Notepad++>net user demo /add
```

The command completed successfully.