AppLocker Bypass – Weak Path Rules

pentestlab.blog/category/red-team/page/114

May 22, 2017

AppLocker rules by default are allowing all the files that are inside in the Windows folder and Program files to be executed as otherwise the system will not operate as normal. If appropriate permissions are not set in these folders an attacker could exploit this in order to bypass AppLocker.

Windows environments (check was done in Windows Server 2008 R2) by default allowing standard users of the system to have read and write access in these folders:

- C:\Windows\Tasks
- C:\Windows\Temp
- C:\Windows\tracing

The accesschk tool can be used to identify if the group “Users” have RW permissions inside the Windows folder.

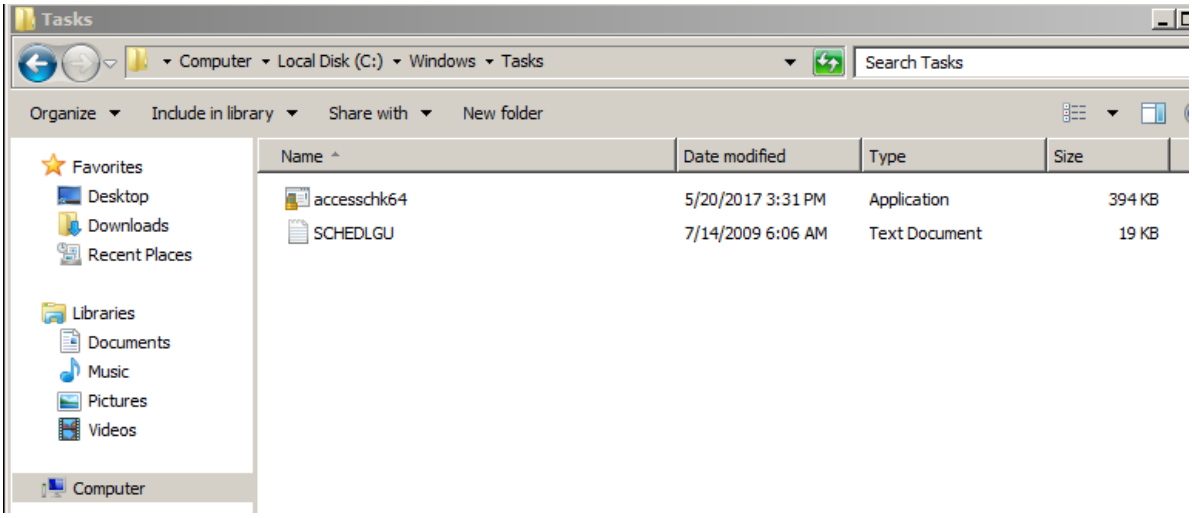
```
C:\>accesschk64.exe "Users" C:\Windows -w

Accesschk v6.10 - Reports effective permissions for securable objects
Copyright (C) 2006-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

RW C:\Windows\Temp
RW C:\Windows\tracing
```

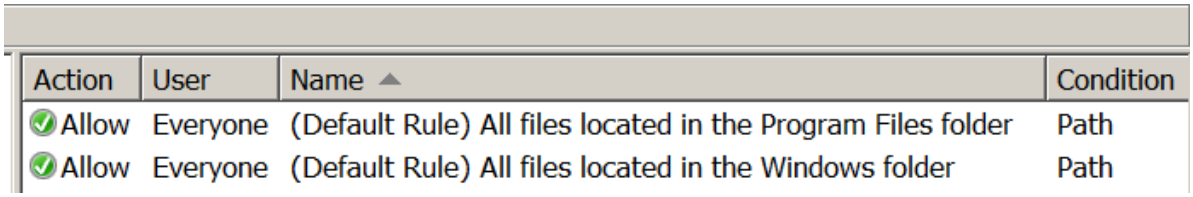
Weak Permissions n Windows Folder

The next step is to drop the binary into the folder that has weak permissions and execute it. In this case the executable is the legitimate application accesschk64.

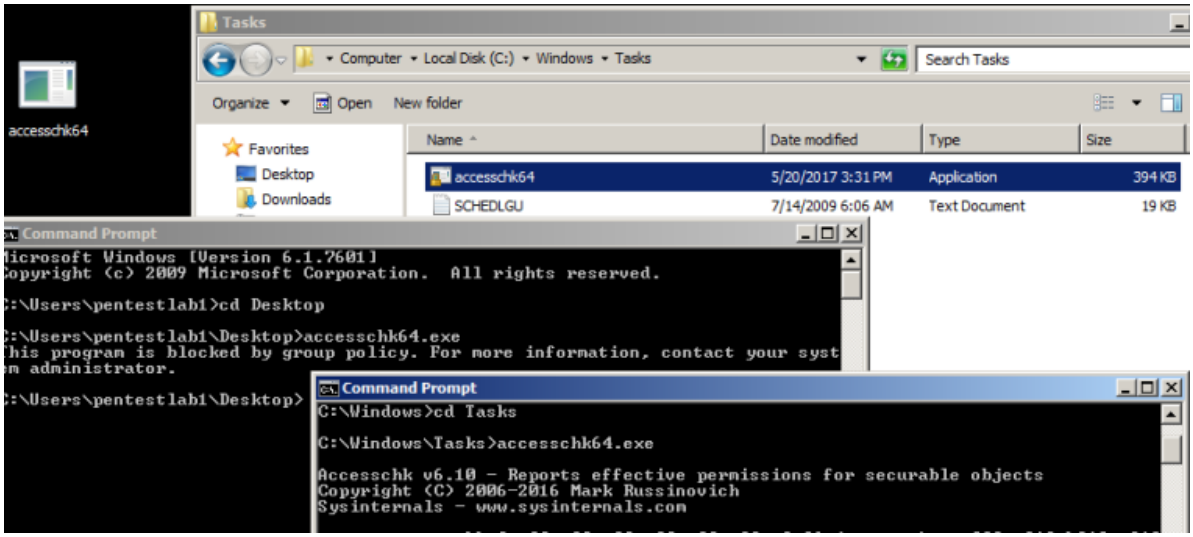


AppLocker – Binary Planting into Weak Folder

Since the AppLocker rules are allowing files that are contained inside the Windows folder to be executed then the utility would run as normal. Otherwise it will be blocked by the AppLocker rules.



AppLocker – Default Rules



AppLocker Bypass – Weak Path Rules

Conclusion

Implementing AppLocker by default doesn't really provide any security measure since it can be bypassed easily. As AppLocker by default trusts Microsoft signed binaries and Windows folders it is essential to evaluate permissions and trusted binaries that can execute code in order to protect effectively the Windows ecosystem.