**Unquoted Service Path**

**“C:\Program Files (x86)\Internet Exp\ExtExport.exe**

**C:\Program Files (x86)\Internet Exp\ExtExport.exe**

* Without the quotes, the prompt will assume the spaces as the delimiter
* Will actually try to run C:\Program instead of C:\Program Files\... which is ran in the top cmd

When running the unquoted path, the prompt will try to execute the cmd in this order:

* C:\Program.exe # can’t find it
* C:\Program Files.exe # can’t find it
* C:\Program Files (x86)\
* C:\Program Files (x86)\internet.exe # will try to execute it as an executable

So in this situation, if we have write access to C:\Program Files (x86), or even C:\Program Files (x86)\Internet Exp\, then we could implant a custom file called Internet.exe to be executed when the path is run unquoted

Wmic service get name,pathname

* Provides list of available services

Text

Description automatically generated

Here we see two services, with spaces, being queried – one quoted and one unquoted

* The unquoted is the one that’s more suitable for our task

Text

Description automatically generated

A program called accesschk.exe can be downloaded and used to show the access privileges of a user

* This shows that builtin users (all users) have RW access to C:\
  + Download version 1.xx if using windows
  + -d # tells prompt to stay with in cwd and not the dirs under it

May want to migrate your meterpreter shell to a different process 9ps) so that it doesn’t die

* Explorer.exe is a good one as it’ll usually have all permissions