



MOBIA is a business technology integrator with over thirty years of experience and 500+ employees across Canada and USA. Our talented bench of technical engineers and trusted advisors deliver process improvements and business transformations within our core pillars of **Cloud**, **Infrastructure**, **Software Development**, **Cybersecurity** and **Broadband & Wireless Services**.

Our inside-out approach allows us to understand business challenges from deep within the organization, mapping the impact as it ripples outward. This insight enables us to create future-proof solutions that maximize results and repeatedly exceed our client's expectations.

Adversary Simulation Workshop

Lab Guide:

Check or Get Prerequisites for Atomic Test

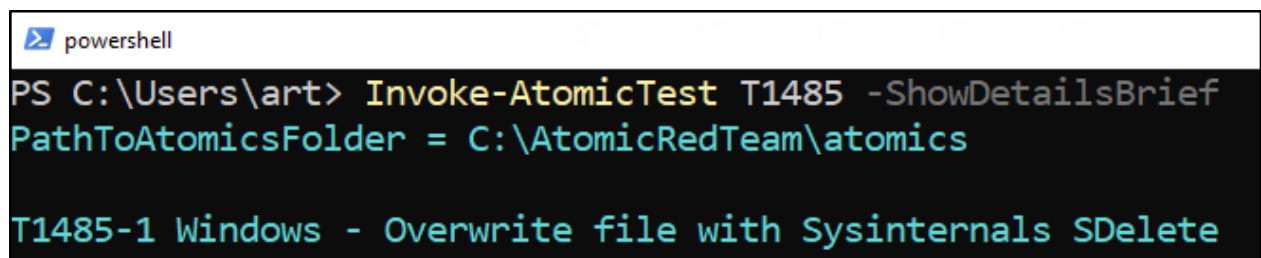
Objective:

Use the execution framework to check if our system meets the prerequisites for executing an atomic test. If dependencies aren't met, use the framework to download, install, or otherwise meet the prerequisites.

Instructions:

Some Atomic Tests have dependencies on certain applications being installed or files being present. The dependencies or “prerequisites” must be satisfied in order to successfully run the atomic test. Let's look at a test under Technique T1485 - Data Destruction.

```
Invoke-AtomicTest T1485 -ShowDetailsBrief
```

A screenshot of a PowerShell terminal window. The title bar shows a blue icon and the text "powershell". The command prompt shows "PS C:\Users\art> Invoke-AtomicTest T1485 -ShowDetailsBrief". Below the command, the output "PathToAtomicsFolder = C:\AtomicRedTeam\atomics" is displayed. At the bottom, the test name "T1485-1 Windows - Overwrite file with Sysinternals SDelete" is shown in a larger font.

```
PS C:\Users\art> Invoke-AtomicTest T1485 -ShowDetailsBrief
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

T1485-1 Windows - Overwrite file with Sysinternals SDelete
```

We will run the first test which securely deletes a file using the Sysinternals SDelete tool. If we try to run this test right off, we will get an error that “sdelete.exe” is not recognized as an operable program. This is because SDelete does not come installed on a default Windows OS.

```
powershell
PS C:\Users\art> Invoke-AtomicTest T1485 -TestNumbers 1
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1485-1 Windows - Overwrite file with Sysinternals SDelete

C:\Users\art\AppData\Local\Temp\Sdelete\sdelete.exe : The term
'C:\Users\art\AppData\Local\Temp\Sdelete\sdelete.exe' is not recognized
as the name of a cmdlet, function, script file, or operable program.
Check the spelling of the name, or if a path was included, verify that
the path is correct and try again.
```

If we take a look at [the markdown file that describes this test](#), we see that there is a prerequisite that the “Secure delete tool from Sysinternals must exist on disk at specified location” and “The file to delete must exist”.

Dependencies: Run with `powershell` !

Description: `Secure delete tool from Sysinternals must exist on disk at specified location ({sdelete_exe})`

Check Prereq Commands:

```
if (Test-Path #{sdelete_exe}) {exit 0} else {exit 1}
```

Get Prereq Commands:

```
Invoke-WebRequest "https://download.sysinternals.com/files/SDelete.zip" -OutFile "$env:TEMP\SDelete.zip"
Expand-Archive $env:TEMP\SDelete.zip $env:TEMP\Sdelete -Force
Remove-Item $env:TEMP\SDelete.zip -Force
```

Description: `The file to delete must exist at {file_to_delete}`

Check Prereq Commands:

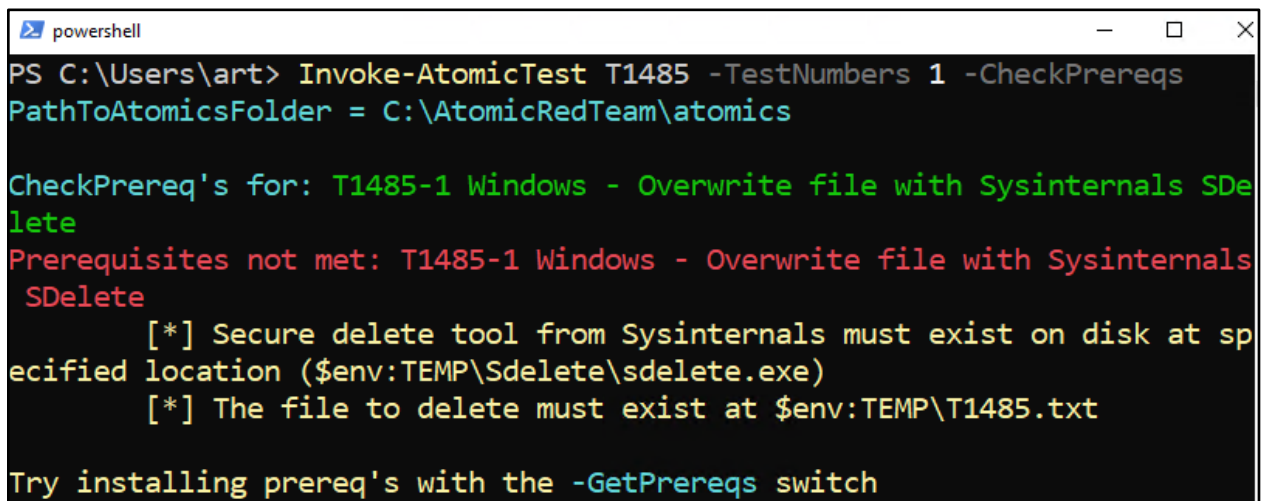
```
if (Test-Path #{file_to_delete}) { exit 0 } else { exit 1 }
```

Get Prereq Commands:

```
New-Item #{file_to_delete} -Force | Out-Null
```

We can use the “CheckPrereqs” flag to check if we meet the prerequisites before running the test.

```
Invoke-AtomicTest T1485 -TestNumbers 1 -CheckPrereqs
```



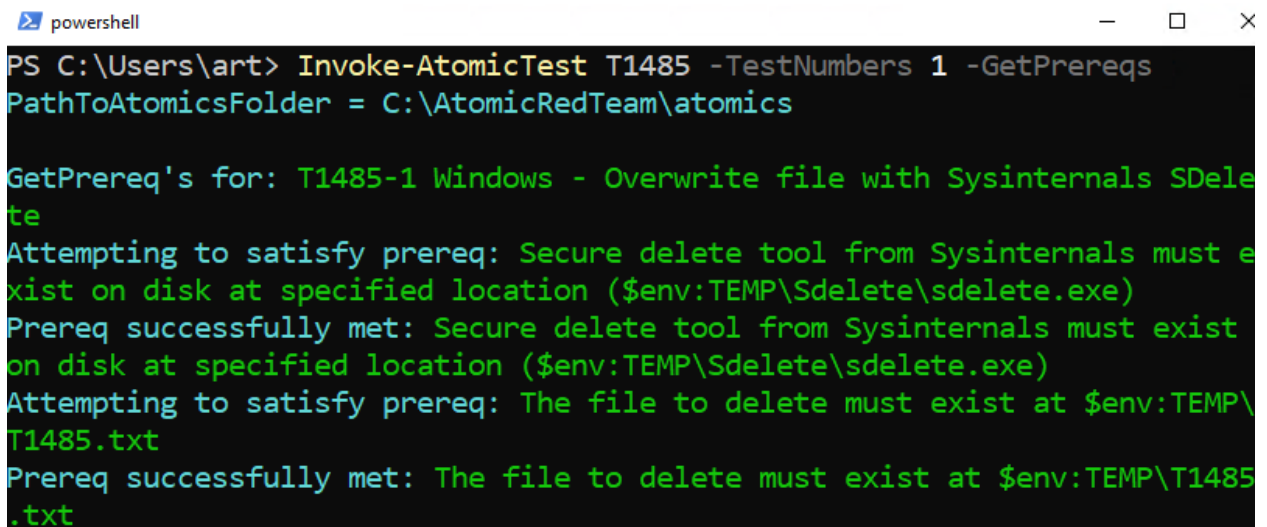
```
PS C:\Users\art> Invoke-AtomicTest T1485 -TestNumbers 1 -CheckPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

CheckPrereq's for: T1485-1 Windows - Overwrite file with Sysinternals SDelete
Prerequisites not met: T1485-1 Windows - Overwrite file with Sysinternals SDelete
    [*] Secure delete tool from Sysinternals must exist on disk at specified location ($env:TEMP\Sdelete\sdelete.exe)
    [*] The file to delete must exist at $env:TEMP\T1485.txt

Try installing prereq's with the -GetPrereqs switch
```

We see that we failed to meet both of the prerequisites. We can then use the “GetPrereqs” flag to meet these dependencies.

```
Invoke-AtomicTest T1485 -TestNumbers 1 -GetPrereqs
```



```
PS C:\Users\art> Invoke-AtomicTest T1485 -TestNumbers 1 -GetPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

GetPrereq's for: T1485-1 Windows - Overwrite file with Sysinternals SDelete
Attempting to satisfy prereq: Secure delete tool from Sysinternals must exist on disk at specified location ($env:TEMP\Sdelete\sdelete.exe)
Prereq successfully met: Secure delete tool from Sysinternals must exist on disk at specified location ($env:TEMP\Sdelete\sdelete.exe)
Attempting to satisfy prereq: The file to delete must exist at $env:TEMP\T1485.txt
Prereq successfully met: The file to delete must exist at $env:TEMP\T1485.txt
```

The output indicates that both prerequisites have been successfully met. We can now successfully execute this test.

```
powershell
PS C:\Users\art> Invoke-AtomicTest T1485 -TestNumbers 1
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1485-1 Windows - Overwrite file with Sysinternals SDelete

Copyright (C) 1999-2018 Mark Russinovich
Sysinternals - www.sysinternals.com

SDelete is set for 1 pass.
C:\Users\art\AppData\Local\Temp\T1485.txt...deleted.

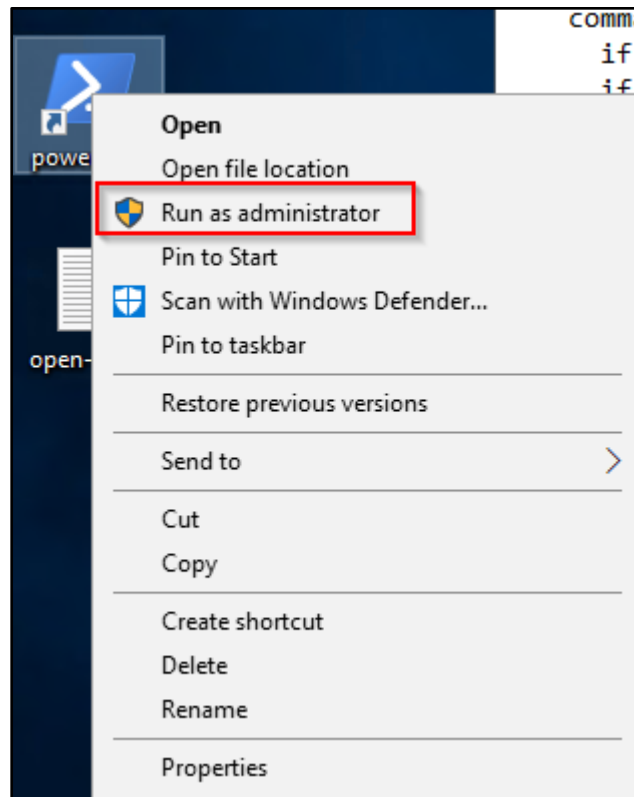
Files deleted: 1
Done executing test: T1485-1 Windows - Overwrite file with Sysinternals SDelete
```

Each atomic test specifies whether elevation is required in order to run the atomic test successfully. If a test requires admin privileges and you run the “CheckPrereq” from an un-elevated context, the execution will report that you failed to meet the prerequisites because “Elevation was required but not provided”.

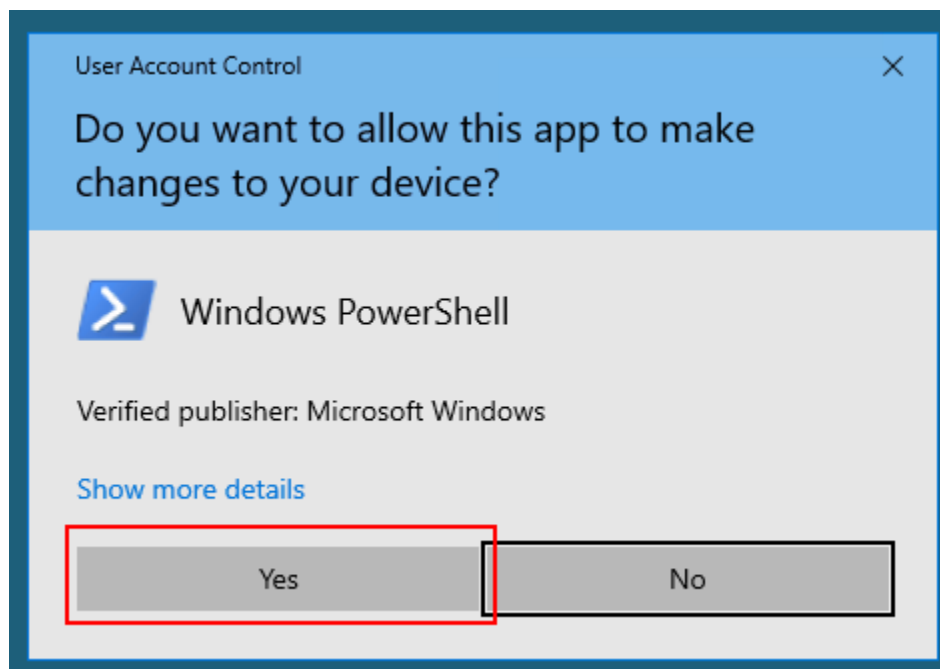
```
PS C:\AtomicRedTeam> Invoke-AtomicTest T1003 -CheckPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

CheckPrereq's for: T1003-1 Powershell Mimikatz
Prerequisites not met: T1003-1 Powershell Mimikatz
[*] Elevation required but not provided
```

To run an atomic test with elevated privileges, you will need to start PowerShell with the “Run as administrator” option. To do this, right click on the PowerShell icon and then click on Run as administrator.



You will need to click “Yes” at the prompt to run as administrator.



Now that we know how to check and satisfy any dependencies for the atomic tests we want to execute we are ready to execute tests!

End of Lab