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:
Cleanup After Test Execution

Objective:

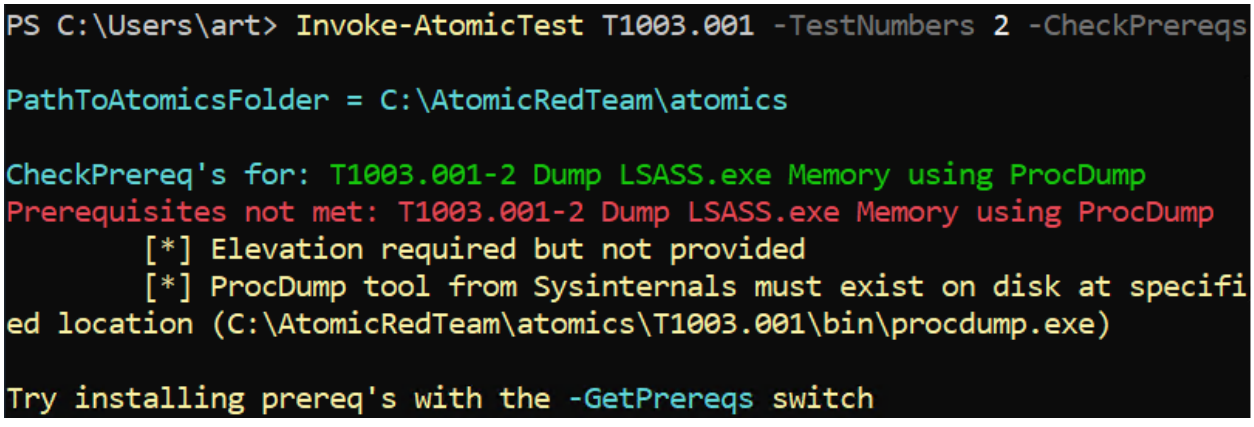
Run the clean up commands defined in the atomic test after executing an atomic test to reset the system and prepare it for executing the test again.

Instructions:

Some atomic tests create files that may contain sensitive information or otherwise clutter up the file system. Other tests may change settings to insecure values or stop services. It is often desirable to delete the files created during atomic test execution or otherwise reset the system to normal operating parameters. Many of the atomic tests include "cleanup_commands" which do exactly that and we can use the execution framework to run these commands.

Let's run through a full example of checking and satisfying prereqs, executing a test, and finally cleaning up. For this we will use The "Dump LSASS.exe Memory using ProcDump" test from T1003.011. First, check the prerequisites.

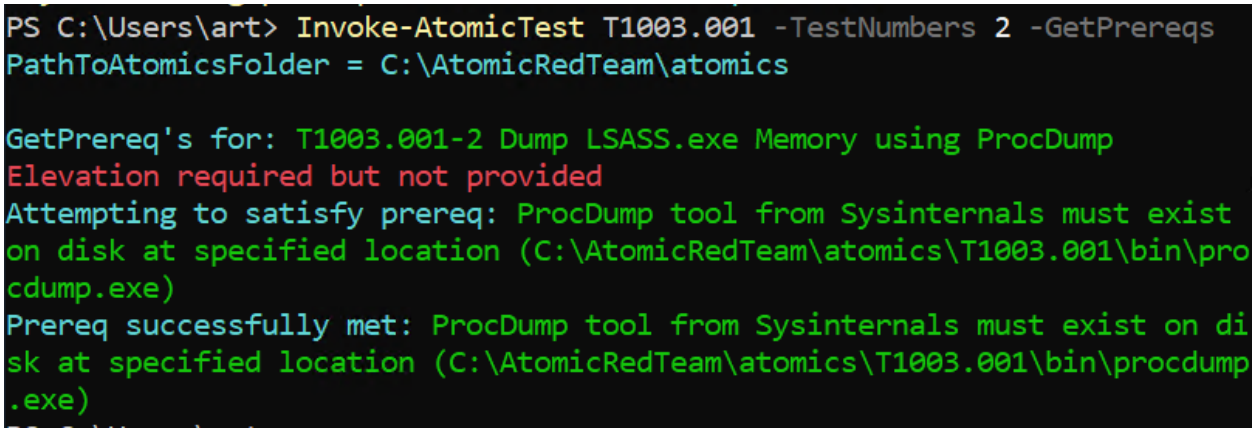
```
Invoke-AtomicTest T1003.001 -TestNumbers 2 -CheckPrereqs
```



As can be seen, in order to run the test to dump the LSASS.exe memory, we need to satisfy two prerequisites. The first can be satisfied by running PowerShell as an administrator. The second prerequisite specifies that the

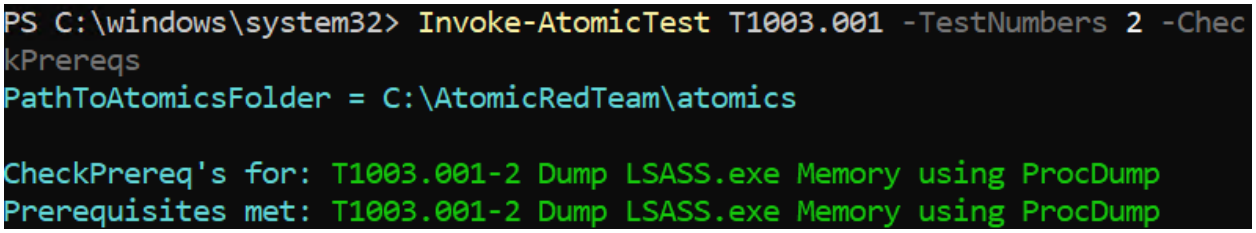
procdump executable must be found at the specified location. In order to get the procdump executable we can run the test with the “GetPrereqs flag, as we did in previous labs.

```
Invoke-AtomicTest T1003.001 -TestNumbers 2 -GetPrereqs
```

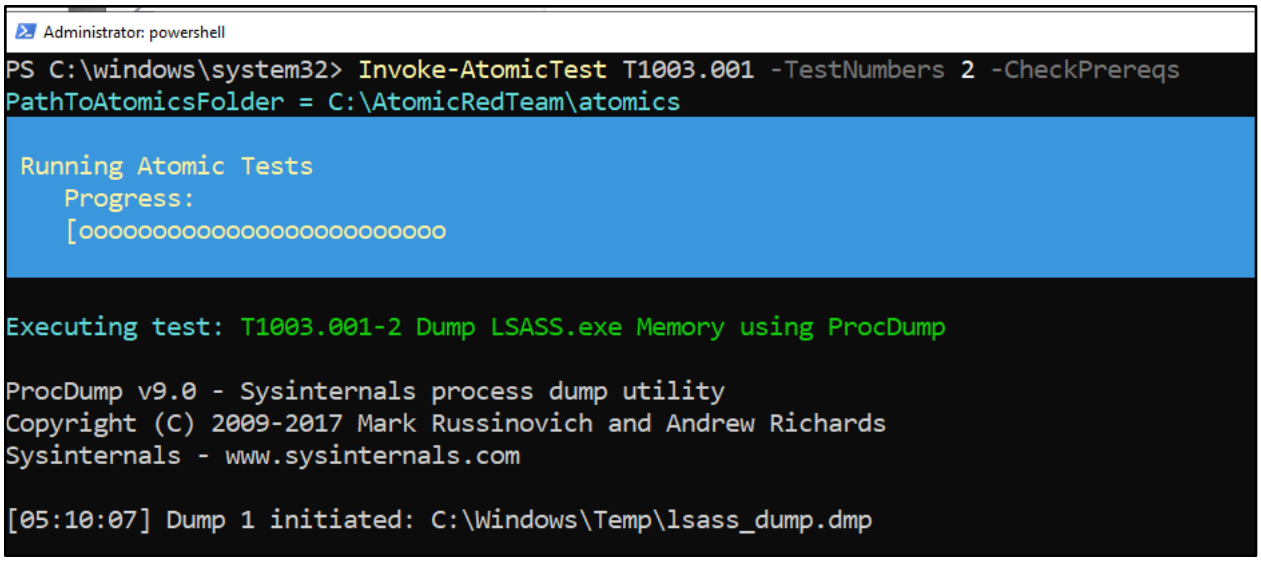


We have now satisfied the second prerequisites but it still complains that elevation is required. To solve this we just need to start PowerShell as an administrator. Right click on the “powershell” shortcut on the desktop and click “Run as administrator”.

Let’s check prerequisites again.

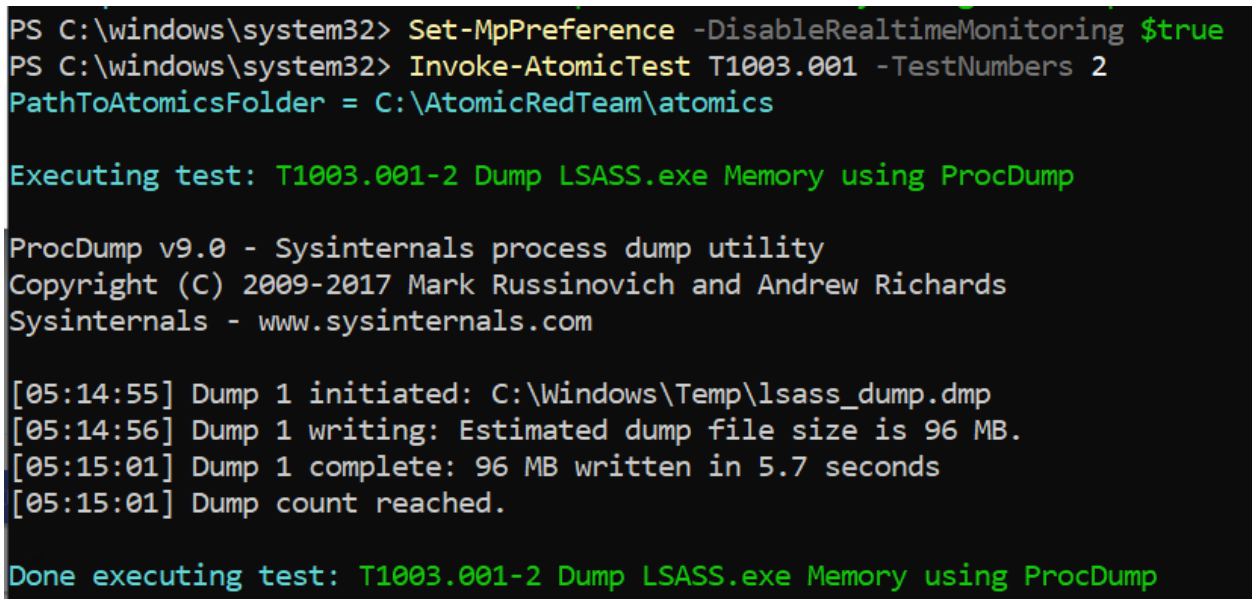


Now that the prerequisites have been met we can run the test.

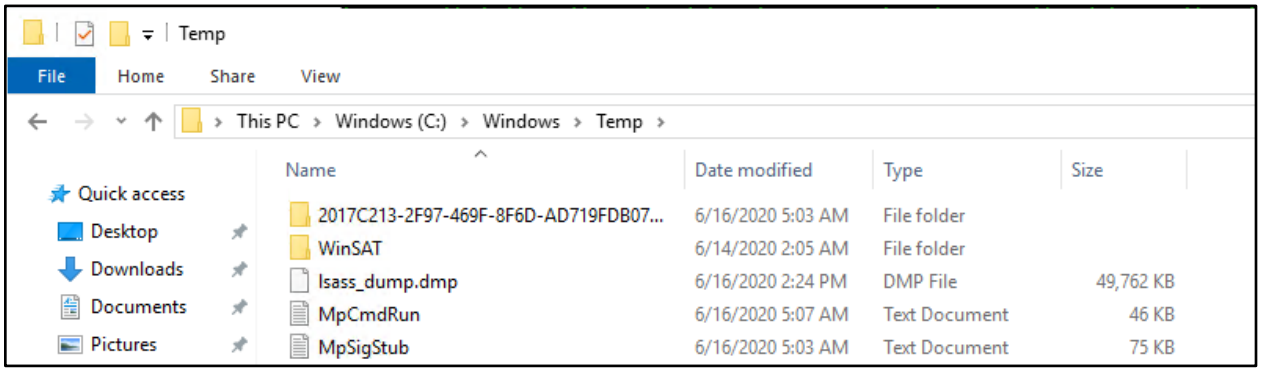


The test hangs because Windows Defender does a good job of blocking this attack attempt. If we want to see the test complete, we will need to temporarily disable Windows Defender.

```
Set-MpPreference -DisableRealtimeMonitoring $true
 Invoke-AtomicTest T1003.001 -TestNumbers 2
```



You can view the lsass dump file in the location indicated - C:\Windows\Temp\lsass_dump.dmp



Sometimes after running Atomic tests there are artifacts that are left over that are sensitive in nature. This is one of those examples. We don't want to leave the dump file laying around. After you have finished the test, you can run the cleanup command to make sure the lsass dump is not left on disk. We can check the details for the test to see what the cleanup command will do.

```
Cleanup Commands:
Command:
del "#{output_file}" >nul 2> nul
Command (with inputs):
del "C:\Windows\Temp\lsass_dump.dmp" >nul 2> nul
```

In order to cleanup after the test, we invoke the test with the "Cleanup" flag

```
Invoke-AtomicTest T1003.001 -TestNumbers 2 -Cleanup
```

```
PS C:\windows\system32> Invoke-AtomicTest T1003.001 -TestNumbers 2 -Cleanup
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing cleanup for test: T1003.001-2 Dump LSASS.exe Memory using ProcDump
Done executing cleanup for test: T1003.001-2 Dump LSASS.exe Memory using ProcDump
```

Look at the location where the file was saved to make sure it has been removed.

```
cat C:\Windows\Temp\lsass_dump.dmp
```

```
PS C:\windows\system32> cat C:\Windows\Temp\lsass_dump.dmp
cat : Cannot find path 'C:\Windows\Temp\lsass_dump.dmp' because it does not exist.
```

Some other useful examples of clean up commands are found here:

- Registry Clean Up
- Re-enable and Start Service
- Delete a User
- Delete a Proxy
- Remove a Registry Key
- Remove Scheduled Tasks

This completes the lab on executing cleanup commands. You have now learned how to use the execution framework to execute atomic tests, including setup, cleanup and custom inputs.

End of Lab