MOBIA

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

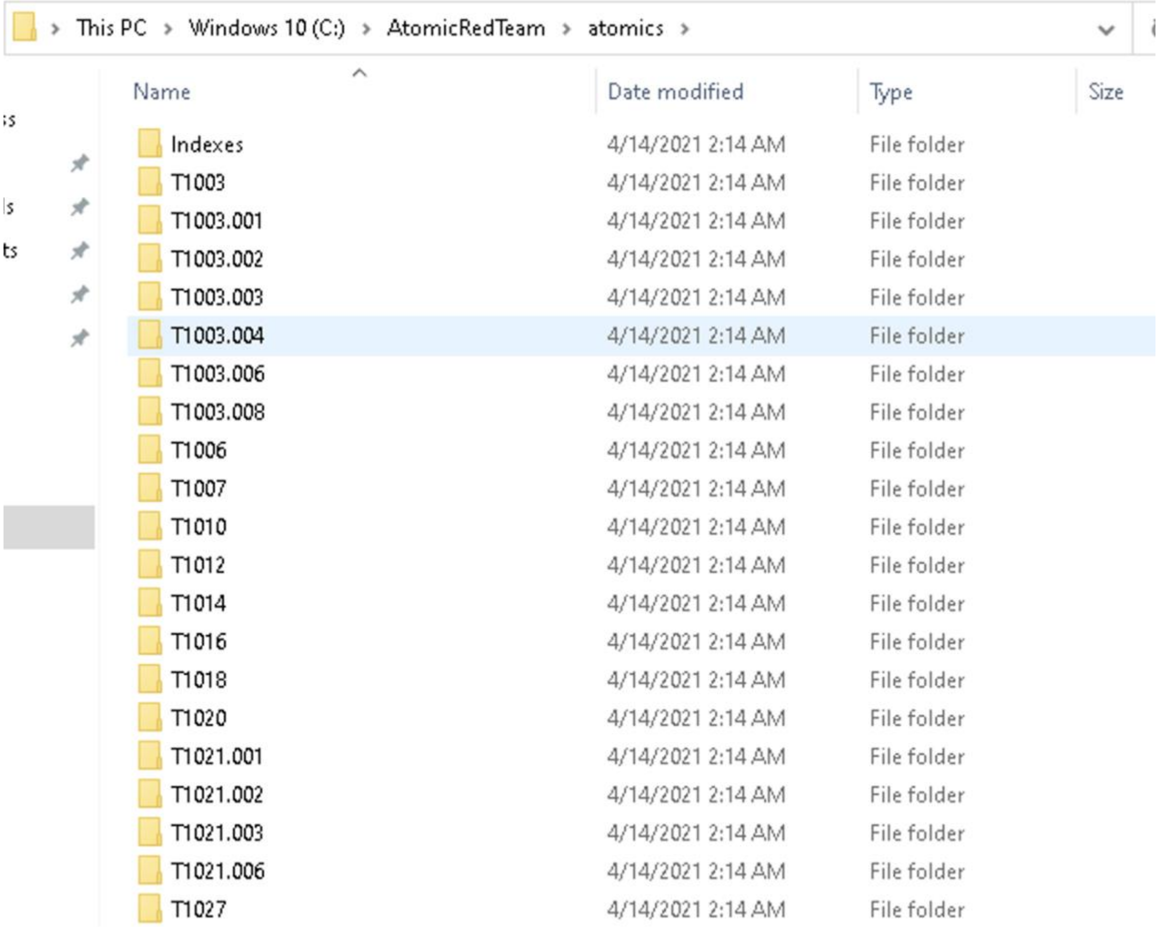
Lab Guide:
Creating an Atomic Test

Objective:

Create an a custom Atomic test.

Instructions:

From your student lab machine navigate open the local atomics folder (C:\AtomicRedTeam\atomics).



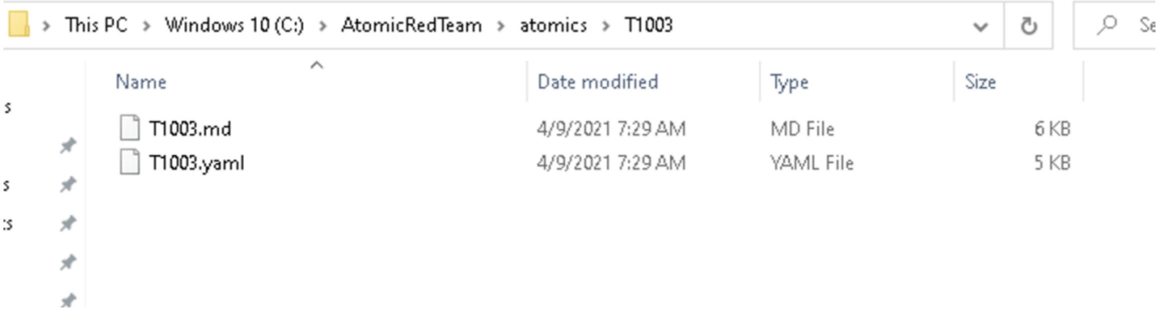
This PC > Windows 10 (C:) > AtomicRedTeam > atomics >

Name	Date modified	Type	Size
Indexes	4/14/2021 2:14 AM	File folder	
T1003	4/14/2021 2:14 AM	File folder	
T1003.001	4/14/2021 2:14 AM	File folder	
T1003.002	4/14/2021 2:14 AM	File folder	
T1003.003	4/14/2021 2:14 AM	File folder	
T1003.004	4/14/2021 2:14 AM	File folder	
T1003.006	4/14/2021 2:14 AM	File folder	
T1003.008	4/14/2021 2:14 AM	File folder	
T1006	4/14/2021 2:14 AM	File folder	
T1007	4/14/2021 2:14 AM	File folder	
T1010	4/14/2021 2:14 AM	File folder	
T1012	4/14/2021 2:14 AM	File folder	
T1014	4/14/2021 2:14 AM	File folder	
T1016	4/14/2021 2:14 AM	File folder	
T1018	4/14/2021 2:14 AM	File folder	
T1020	4/14/2021 2:14 AM	File folder	
T1021.001	4/14/2021 2:14 AM	File folder	
T1021.002	4/14/2021 2:14 AM	File folder	
T1021.003	4/14/2021 2:14 AM	File folder	
T1021.006	4/14/2021 2:14 AM	File folder	
T1027	4/14/2021 2:14 AM	File folder	

Notice the structure of this directory, if you haven't noticed this in previous labs each of the test names is structure as follows:

C:\AtomicRedTeam\atomics\<TestName>\<TestName>.yaml
C:\AtomicRedTeam\atomics\<TestName>\<TestName>.md

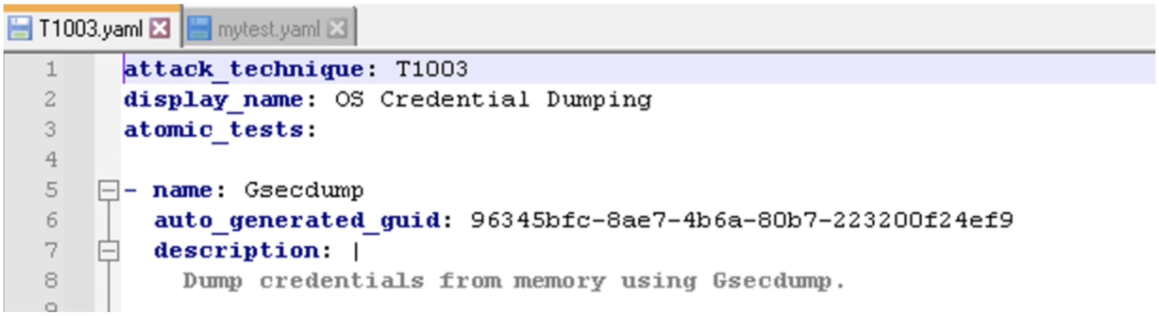
For example look at T1003:



Name	Date modified	Type	Size
T1003.md	4/9/2021 7:29 AM	MD File	6 KB
T1003.yaml	4/9/2021 7:29 AM	YAML File	5 KB

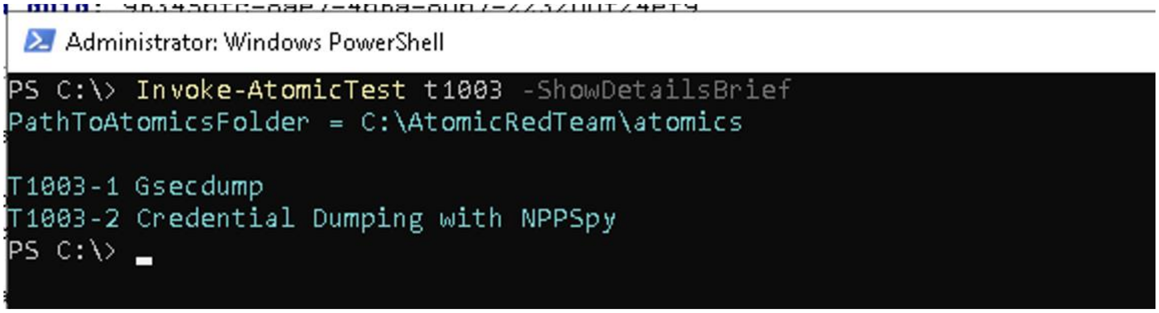
The *.md file is the description of the test and the *.yaml is the execution plan.

Open the *.yaml file from T1003 in notepad and review the first 3 lines of the file:



```
attack_technique: T1003
display_name: OS Credential Dumping
atomic_tests:

- name: Gsecdump
  auto_generated_guid: 96345bfc-8ae7-4b6a-80b7-223200f24ef9
  description: |
    Dump credentials from memory using Gsecdump.
```

These first few lines provide a test name and display name, like we see in the output of -ShowDetailsBrief:



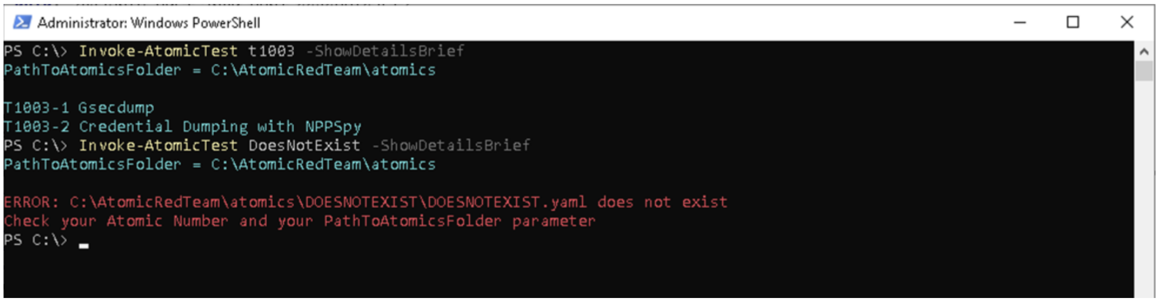
```
PS C:\> Invoke-AtomicTest t1003 -ShowDetailsBrief
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

T1003-1 Gsecdump
T1003-2 Credential Dumping with NPPSpy
PS C:\> _
```

Notice that the PathToAtomicsFolder is displayed at the top showing the default path.

Run the following command the review the output:

Invoke-AtomicTest DoesNotExist -ShowDetailsBrief

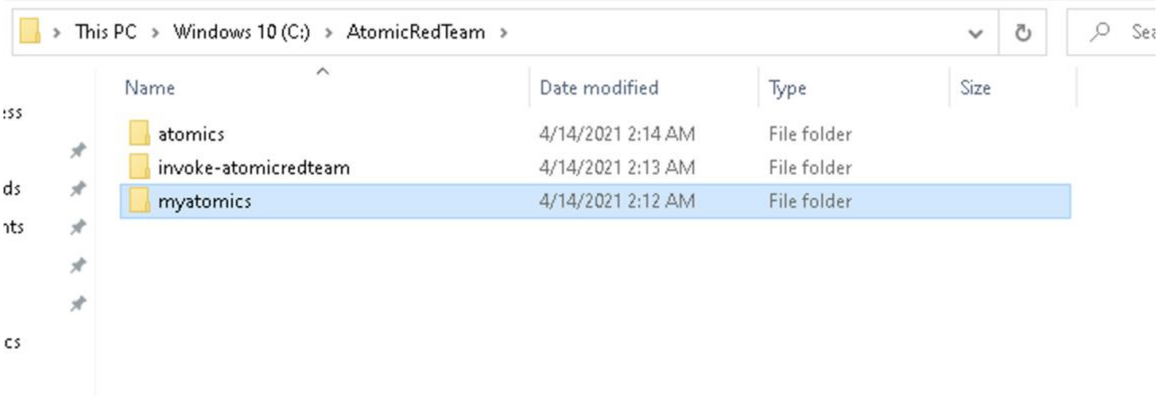
The result is as follows:



```
PS C:\> Invoke-AtomicTest t1003 -ShowDetailsBrief
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

T1003-1 Gsecdump
T1003-2 Credential Dumping with NPPSpy
PS C:\> Invoke-AtomicTest DoesNotExist -ShowDetailsBrief
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

ERROR: C:\AtomicRedTeam\atomics\DOESNOTEXIST\DOESNOTEXIST.yaml does not exist
Check your Atomic Number and your PathToAtomicsFolder parameter
PS C:\> _
```

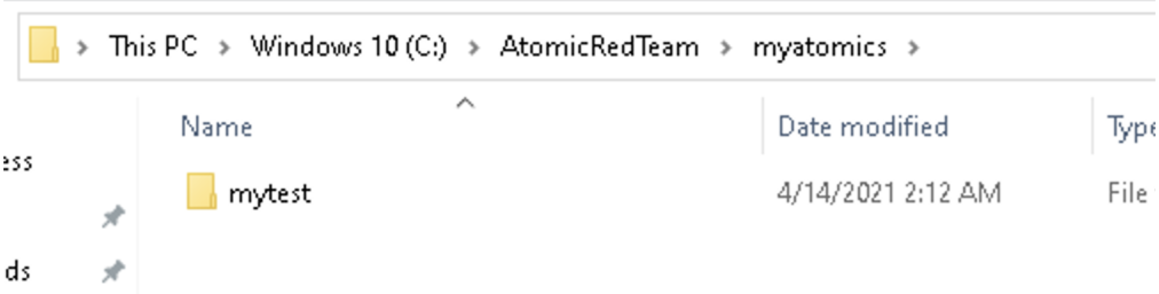
We can see in the error that Invoke-AtomicTest is trying to find the folder and *.md/*.yaml files in our atomics folder.

Let’s create a basic atomic test. First create a new directory outside the atomics folder to work in: C:\AtomicRedTeam\myatomics



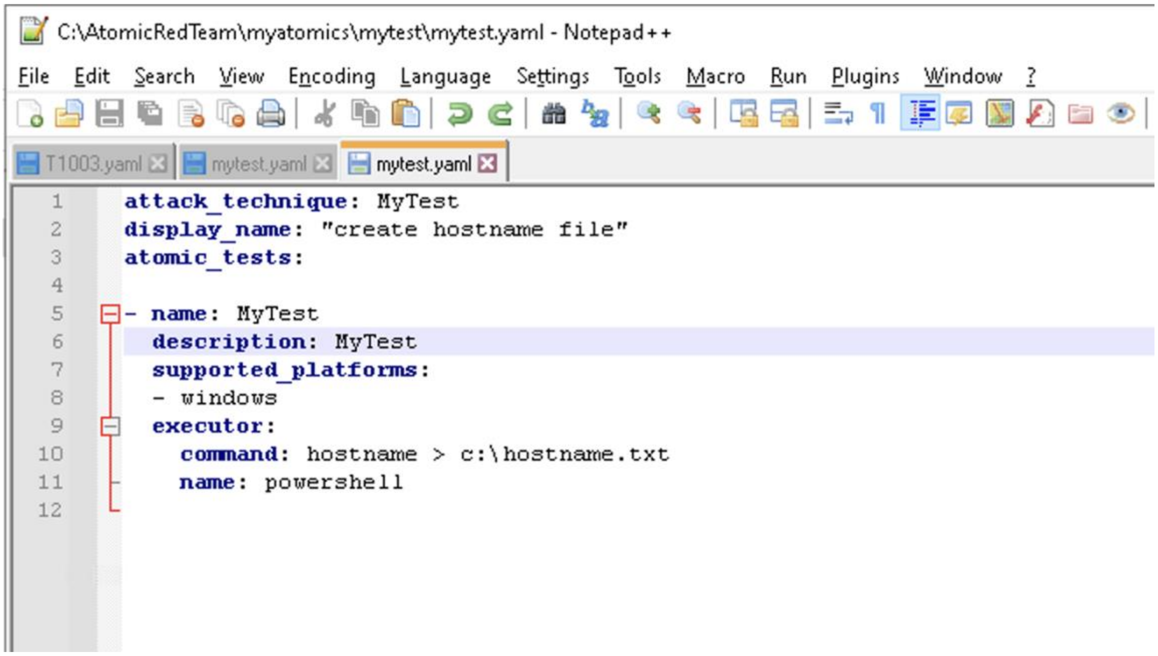
Name	Date modified	Type	Size
atomics	4/14/2021 2:14 AM	File folder	
invoke-atomicredteam	4/14/2021 2:13 AM	File folder	
myatomics	4/14/2021 2:12 AM	File folder	

Now under the myatomics folder create your new atomic test. We’ll use the test mytest:



Name	Date modified	Type
mytest	4/14/2021 2:12 AM	File

Under the mytest folder create the file mytest.yaml with the following content:

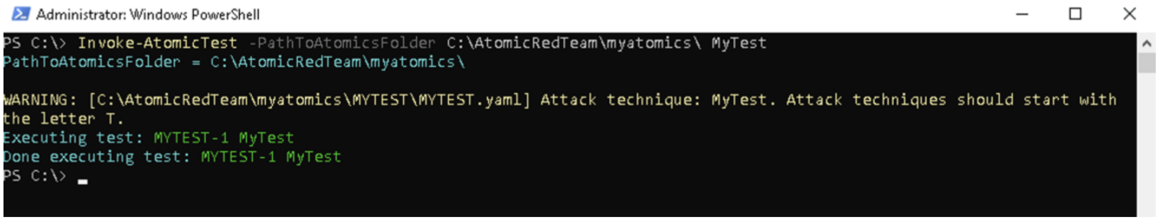

C:\AtomicRedTeam\myatomics\mytest\mytest.yaml - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
T1003.yaml
mytest.yaml
mytest.yaml

```
attack_technique: MyTest
display_name: "create hostname file"
atomic_tests:

- name: MyTest
  description: MyTest
  supported_platforms:
  - windows
  executor:
    command: hostname > c:\hostname.txt
    name: powershell
```

```
attack_technique: MyTest
display_name: "create hostname file"
atomic_tests:

- name: MyTest
  description: MyTest
  supported_platforms:
  - windows
  executor:
    command: hostname > c:\hostname.txt
    name: powershell
```

Save the file and run the following command to execute your newly created test:

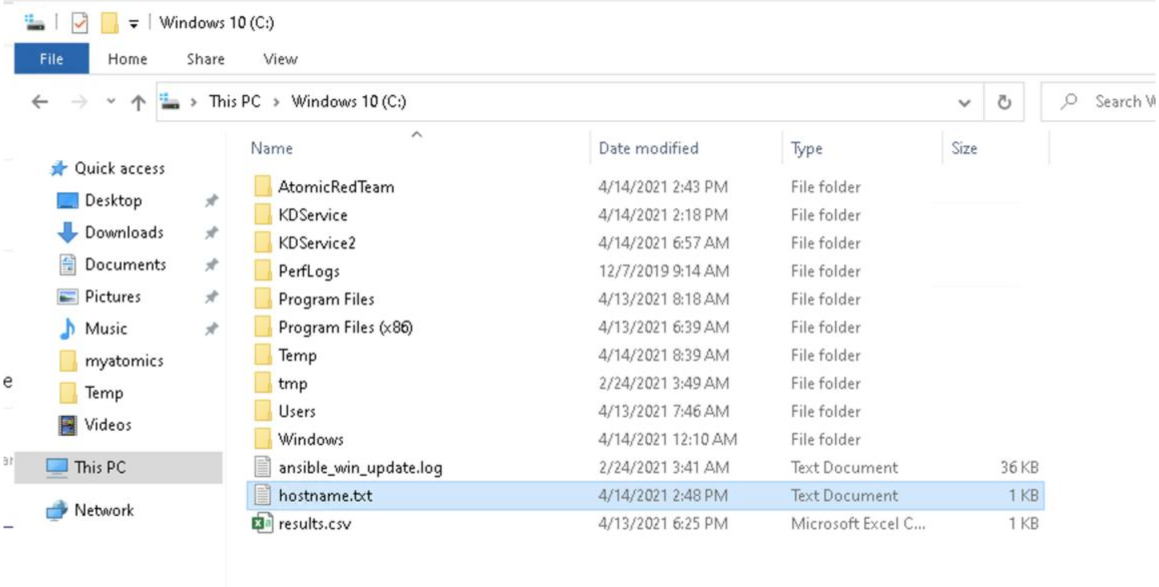
Invoke-AtomicTest -PathToAtomicsFolder C:\AtomicRedTeam\myatomics\ MyTest



```
PS C:\> Invoke-AtomicTest -PathToAtomicsFolder C:\AtomicRedTeam\myatomics\ MyTest
PathToAtomicsFolder = C:\AtomicRedTeam\myatomics\

WARNING: [C:\AtomicRedTeam\myatomics\MYTEST\MYTEST.yaml] Attack technique: MyTest. Attack techniques should start with
the letter T.
Executing test: MYTEST-1 MyTest
Done executing test: MYTEST-1 MyTest
PS C:\> _
```

You'll receive a warning but that's ok to ignore for now. When submitting to the atomicredteam project there are some more strict guidelines on formatting.

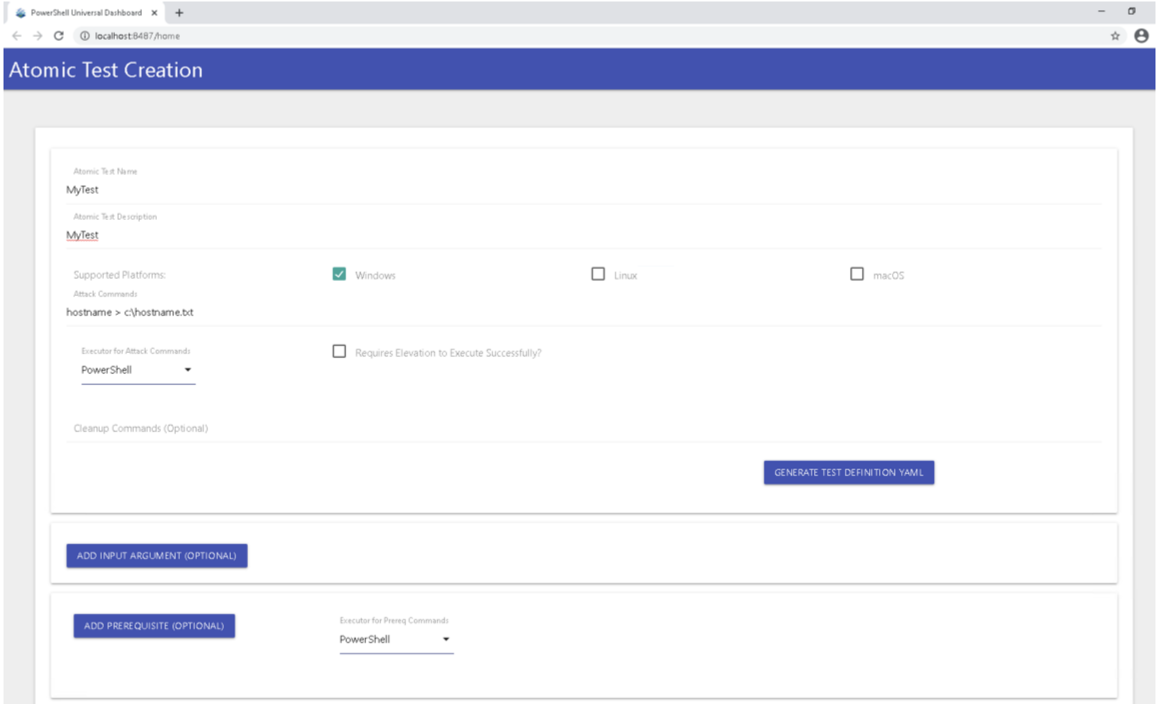
Check to see that the hostname.txt file was created under c:\



Name	Date modified	Type	Size
AtomicRedTeam	4/14/2021 2:43 PM	File folder	
KDService	4/14/2021 2:18 PM	File folder	
KDService2	4/14/2021 6:57 AM	File folder	
PerfLogs	12/7/2019 9:14 AM	File folder	
Program Files	4/13/2021 8:18 AM	File folder	
Program Files (x86)	4/13/2021 6:39 AM	File folder	
Temp	4/14/2021 8:39 AM	File folder	
tmp	2/24/2021 3:49 AM	File folder	
Users	4/13/2021 7:46 AM	File folder	
Windows	4/14/2021 12:10 AM	File folder	
ansible_win_update.log	2/24/2021 3:41 AM	Text Document	36 KB
hostname.txt	4/14/2021 2:48 PM	Text Document	1 KB
results.csv	4/13/2021 6:25 PM	Microsoft Excel C...	1 KB

One other tool that is available, if you don't have something like notepad++ or you'd like to more closely follow formatting guidelines during test is the Start-AtomicGui web interface.

To launch, execute Start-AtomicGui from your powershell prompt. After a minute or so you should see the following:


PowerShell Universal Dashboard
localhost:8487/home
GENERATE TEST DEFINITION YAML
ADD INPUT ARGUMENT (OPTIONAL)
ADD PREREQUISITE (OPTIONAL)

Atomic Test Creation

Atomic Test Name: MyTest

Atomic Test Description: MyTest

Supported Platforms: ☑ Windows ☐ Linux ☐ macOS

Attack Commands: hostname > c:\hostname.txt

Executor for Attack Commands: PowerShell

☐ Requires Elevation to Execute Successfully?

Cleanup Commands (Optional)

Executor for Prereq Commands: PowerShell

End of Lab