Atomic red team from RedCanary

Monday, January 2, 2023 11:14 AM

 # By: Abdullah Ali Alhakami |
 # Twitter: @Alhakami1 |===
==========

What is *Atomic red team* from RedCanary? Atomic Red Team™ is a library of simple tests(over 200 different attack techniques) that every security team can execute to test their defenses.
- More about atomic red team

What is *invoke-atomic* from RedCanary? a PowerShell-based framework for developing and executing Atomic Red Team tests.
- Download instruction

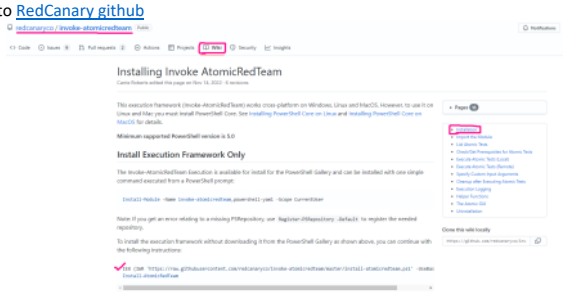
Differences are Atomic Red Team is a collection of detection tests, while Invoke-Atomic is a tool for executing those tests and interacting with the results.

Requirement:
- permission to run tests
- Execute atomics in a lab environment
- PowerShell 5.0 or later | **open PowerShell - $PSVersionTable**

Install Invoke-Atomic:

1. Go to RedCanary github

i.



ii. Execute the command.

1) Error might arise "Execution-Policy is disabled". Execution policy is part of PowerShell security strategy. For example, determine whether you can load configuration files, such as your PowerShell profile, or run scripts. And, whether scripts must be digitally signed before they are run.

```
Installation of AtomicRedTeam failed.
File C:\Users\Administrator\Documents\WindowsPowerShell\Modules\powershell-yaml\0.4.3\Load-Assemblies.ps1 cannot be loaded because running scri
pts is disabled on this system. For more information, see about_Execution_Policies at https:/go.microsoft.com/fwlink/?LinkID=135170.
```

a) First Solution

i) First list the execution policy to make sure its undefined and the problem from it.

```
PS C:\Windows\system32> Get-ExecutionPolicy -List

        Scope ExecutionPolicy
        ----- ---------------
MachinePolicy       Undefined
   UserPolicy       Undefined
      Process       Undefined
  CurrentUser       Undefined
 LocalMachine       Undefined
```

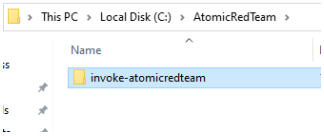
ii) Set an remote signed execution policy and verify.

```
PS C:\Windows\system32> Set-ExecutionPolicy RemoteSigned -Scope LocalMachine

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose
you to the security risks described in the about_Execution_Policies help topic at
https:/go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "N"): y
PS C:\Windows\system32> Get-ExecutionPolicy -List

        Scope ExecutionPolicy
        ----- ---------------
MachinePolicy       Undefined
   UserPolicy       Undefined
      Process       Undefined
  CurrentUser       Undefined
 LocalMachine    RemoteSigned
```

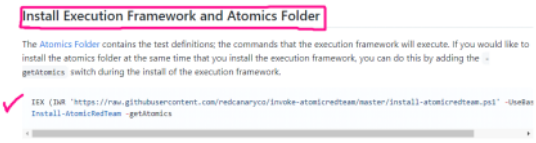
b) Second solution: Create a GPO to change Active Directory PowerShell execution policy

i) Create a new Active Directory GPO
ii) Open the GPO for editing.
iii) In the GPO editor, select Computer Configuration > Policies > Administrative Templates > Windows Components > Windows PowerShell.
iv) Right-click "Turn on script execution", then select "Edit".
v) In the window that appears, click the "Enabled" radio button.
vi) In the "Execution Policy" drop-down, select Allow local scripts and remote signed scripts.

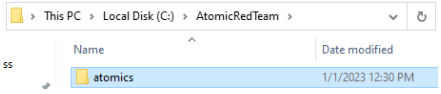
vii) Click "OK" to accept the changes.
viii) Close the Group Policy Object editor to save your changes.
ix) Deploy the GPO.

2. Verify
   i. From the command prompt:
   ✧
   ```
   Installation of Invoke-AtomicRedTeam is complete. You can now use the Invoke-AtomicTest function
   See Wiki at https://github.com/redcanaryco/invoke-atomicredteam/wiki for complete details
   PS C:\Windows\system32>
   ```
   ii. Check the C: directory you will find the AtomicRecTeam\invoke-atomicredteam
   ✧
   

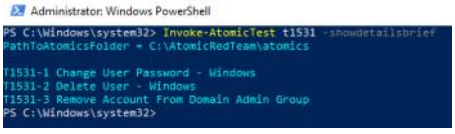
Installing directory of atomic test (Contain over 200 attack techniques)

1. Go to RedCanary github
   ✧
   

   Note: if this command didn't work so execution framework or the atomics folder are already found on disk you must use the-Force parameter during install. Just add -Force next of the above command.

2. Verify
   i. From the command prompt:
   ✧
   ```
   Installation of Invoke-AtomicRedTeam is complete. You can now use the Invoke-AtomicTest function
   See Wiki at https://github.com/redcanaryco/invoke-atomicredteam/wiki for complete details
   ```
   ii. Check the C: directory you will found the AtomicRecTeam inside atomics folder you will found the MITRE-ATT&CK techniques
   ✧
   

Importing the PowerShell Module

1. In order to use Invoke-Atomic we have to import its module into the PowerShell session. But first let's explain what do we mean by module you can think of it like a library in python, to use the function and the variable inside that library you have to import it first. The same idea as here.
   i. Command
   ```
   Import-Module "C:\AtomicRedTeam\invoke-atomicredteam\Invoke-AtomicRedTeam.psd1" -Force
   ```
   Note:
   - You can get the same command from here
   - The PATH depend on where you are storing the AtomicRedTeam.
2. Verify
   i. Let's verify our work by checking details of specific technique. Command:
   ```
   invoke-atomic t# -showdetailsbrief
   ```
   

Listing Atomics with Invoke-Atomic (list the Technique numbers and test names available for execution)

1. To see the techniques details we can use Invoke-AtomicTest with the help of Atomic tests directory as it presented below.
   i. ShowDetailsBrief
   ✧
   ```
   PS C:\Windows\system32> Invoke-AtomicTest t1027 -ShowDetailsBrief
   PathToAtomicsFolder = C:\AtomicRedTeam\atomics

   T1027-2 Execute base64-encoded PowerShell
   T1027-3 Execute base64-encoded PowerShell from Windows Registry
   T1027-4 Execution from Compressed File
   T1027-5 DLP Evasion via Sensitive Data in VBA Macro over email
   T1027-6 DLP Evasion via Sensitive Data in VBA Macro over HTTP
   T1027-7 Obfuscated Command in PowerShell
   PS C:\Windows\system32>
   ```
   ii. ShowDetails

```
PS C:\Windows\system32> Invoke-AtomicTest t1027 -ShowDetails
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

[********BEGIN TEST*******]
Technique: Obfuscated Files or Information T1027
Atomic Test Name: Execute base64-encoded PowerShell
Atomic Test Number: 2
Atomic Test GUID: a50d5a97-2531-499e-a1de-5544c74432c6
Description: Creates base64-encoded PowerShell code and executes it. This is used by numerous adversaries and malicious
tools.
Upon successful execution, powershell will execute an encoded command and stdout default is "Write-Host "Hey, Atomic!"

Attack Commands:
Executor: powershell
ElevationRequired: False
Command:
$OriginalCommand = '#{powershell_command}'
$Bytes = [System.Text.Encoding]::Unicode.GetBytes($OriginalCommand)
$EncodedCommand =[Convert]::ToBase64String($Bytes)
$EncodedCommand
powershell.exe -EncodedCommand $EncodedCommand
Command (with inputs):
$OriginalCommand = 'Write-Host "Hey, Atomic!"'
$Bytes = [System.Text.Encoding]::Unicode.GetBytes($OriginalCommand)
$EncodedCommand =[Convert]::ToBase64String($Bytes)
$EncodedCommand
powershell.exe -EncodedCommand $EncodedCommand
[!!!!!!!!END TEST!!!!!!!]


[********BEGIN TEST*******]
```

Get Prerequisites/dependencies for Atomic Tests in order to preform ready environment for the execution

1. There are several ways to check the dependency of the technique as it presented below.
   i. First way is by going to the technique file and go through the .yaml file (The configuration file of that technique) until you find the dependency section

```
40  dependencies:
41  - description: |
42      Check if netstat command exists on the machine
43    prereq_command: |
44      if [ -x "$(command -v netstat)" ]; then exit 0; else exit 1; fi;
45    get_prereq_command: |
46      echo "Install netstat on the machine."; exit 1;
47  executor:
48    command: |
49      netstat
50      who -a
51    name: sh
```

2. Check the technique details (ShowDetails) as we explained in the "Listing Atomics with Invoke-Atomic".
3. Check a specific technique (Sub technique for a technique)
   i. By applying ShowDetailsBrief and specify a specific one. It will show you the dependency and whether we are meeting it or no.

1)
```
PS C:\Windows\system32> Invoke-AtomicTest t1027 -ShowDetailsBrief
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

T1027-2 Execute base64-encoded PowerShell
T1027-3 Execute base64-encoded PowerShell from Windows Registry
T1027-4 Execution from Compressed File
T1027-5 DLP Evasion via Sensitive Data in VBA Macro over email
T1027-6 DLP Evasion via Sensitive Data in VBA Macro over HTTP
T1027-7 Obfuscated Command in PowerShell
PS C:\Windows\system32> Invoke-AtomicTest t1027 -TestNumbers 6 -CheckPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

CheckPrereq's for: T1027-6 DLP Evasion via Sensitive Data in VBA Macro over HTTP
Prerequisites met: T1027-6 DLP Evasion via Sensitive Data in VBA Macro over HTTP
PS C:\Windows\system32>
```

4. Checking all the above sub techniques we can just remove the -TestNumber option.

i.
```
PS C:\Windows\system32> Invoke-AtomicTest t1027 -CheckPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

CheckPrereq's for: T1027-2 Execute base64-encoded PowerShell
Prerequisites met: T1027-2 Execute base64-encoded PowerShell
CheckPrereq's for: T1027-3 Execute base64-encoded PowerShell from Windows Registry
Prerequisites met: T1027-3 Execute base64-encoded PowerShell from Windows Registry
CheckPrereq's for: T1027-4 Execution from Compressed File
Prerequisites not met: T1027-4 Execution from Compressed File
        [*] T1027.exe must exist on disk at $env:temp\temp_T1027.zip\T1027.exe

Try installing prereq's with the -GetPrereqs switch
CheckPrereq's for: T1027-5 DLP Evasion via Sensitive Data in VBA Macro over email
Prerequisites met: T1027-5 DLP Evasion via Sensitive Data in VBA Macro over email
CheckPrereq's for: T1027-6 DLP Evasion via Sensitive Data in VBA Macro over HTTP
Prerequisites met: T1027-6 DLP Evasion via Sensitive Data in VBA Macro over HTTP
CheckPrereq's for: T1027-7 Obfuscated Command in PowerShell
Prerequisites met: T1027-7 Obfuscated Command in PowerShell
```

5. .

NOTE: if red error show as below, it means the sub technique is only work with linux/other OS

⊙ To satisfy the perquisites we can easily just install/GET it!

```
PS C:\Windows\system32> Invoke-AtomicTest t1027 -TestNumbers 4 -GetPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

GetPrereq's for: T1027-4 Execution from Compressed File
Attempting to satisfy prereq: T1027.exe must exist on disk at $env:temp\temp_T1027.zip\T1027.exe
Prereq successfully met: T1027.exe must exist on disk at $env:temp\temp_T1027.zip\T1027.exe
PS C:\Windows\system32>
```

⊙ In some cases, it require you to do it manually. However, it won't be a problem.

```
Attempting to satisfy prereq: Computer must be domain joined
Joining this computer to a domain must be done manually
Failed to meet prereq: Computer must be domain joined
```

Execute Atomic Tests

Finally, we reached to the most excited part -_-

1. Executing a test/technique is very simple. All what we have to do is writing the attack technique and t

```
PS C:\Windows\system32> Invoke-AtomicTest t1027 -ShowDetailsBrief
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

T1027-2 Execute base64-encoded PowerShell
T1027-3 Execute base64-encoded PowerShell from Windows Registry
T1027-4 Execution from Compressed File
T1027-5 DLP Evasion via Sensitive Data in VBA Macro over email
T1027-6 DLP Evasion via Sensitive Data in VBA Macro over HTTP
T1027-7 Obfuscated Command in PowerShell
PS C:\Windows\system32> Invoke-AtomicTest t1027 -TestNumbers 7
```

```
PS C:\Windows\system32> Invoke-AtomicTest t1027 -ShowDetailsBrief
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

T1027-2 Execute base64-encoded PowerShell
T1027-3 Execute base64-encoded PowerShell from Windows Registry
T1027-4 Execution from Compressed File
T1027-5 DLP Evasion via Sensitive Data in VBA Macro over email
T1027-6 DLP Evasion via Sensitive Data in VBA Macro over HTTP
T1027-7 Obfuscated Command in PowerShell
PS C:\Windows\system32> Invoke-AtomicTest t1027 -TestNumbers 2,5,6
```

2. To run all the sub techniques all you have to do is writing the technique next of Invoke-AtomixTest.

```
PS C:\Windows\system32> Invoke-AtomicTest t1027
```

Specify Custom Input Arguments

- We do mean that we can change the test input argument. For example, if the technique run a specific process or specific payload to be executed. We can change the path of that payload to whatever we want and the same with process, This also can be apply to:
  i. Change filenames
  ii. Customize file path
  iii. Replacing processes
  iv. Modify Process ID

1. How to know what is the input arguments It can be changed in that technique?
   i. Using "ShowDetails" and focused on the RED text (Which indicate that this parameter can be changed).

```
[********BEGIN TEST********]
Technique: Obfuscated Files or Information T1027
Atomic Test Name: Execut base64-encoded PowerShell
Atomic Test Number: 2
Atomic Test GUID: a50d5a97-2531-499e-a1de-5544c74432c6
Description: Creates base64-encoded PowerShell code and executes it
tools.
Upon successful execution, powershell will execute an encoded comm

Attack Commands:
Executor: powershell
ElevationRequired: False
Command:
$OriginalCommand = '#{powershell_command}'
$Bytes = [System.Text.Encoding]::Unicode.GetBytes($OriginalCommand)
$EncodedCommand =[Convert]::ToBase64String($Bytes)
$EncodedCommand
powershell.exe -EncodedCommand $EncodedCommand
Command (with inputs):
$OriginalCommand = 'Write-Host "Hey, Atomic!"'
$Bytes = [System.Text.Encoding]::Unicode.GetBytes($OriginalCommand)
$EncodedCommand =[Convert]::ToBase64String($Bytes)
$EncodedCommand
powershell.exe -EncodedCommand $EncodedCommand
[!!!!!!!!END TEST!!!!!!!!]
```

   ii. Now we will use the below command to change the parameter.

```
PS C:\Windows\system32> Invoke-AtomicTest t1027 -ShowDetailsBrief
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

T1027-2 Execute base64-encoded PowerShell
T1027-3 Execute base64-encoded PowerShell from Windows Registry
T1027-4 Execution from Compressed File
T1027-5 DLP Evasion via Sensitive Data in VBA Macro over email
T1027-6 DLP Evasion via Sensitive Data in VBA Macro over HTTP
T1027-7 Obfuscated Command in PowerShell
PS C:\Windows\system32> Invoke-AtomicTest t1027 -TestNumbers 2 -PromptForInputArgs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Enter a value for powershell_command , or press enter to accept the default.
PowerShell command to encode [Write-Host "Hey, Atomic!"]: what ever you want
```

Cleanup After the mess

- Many atomic tests include cleanup commands to remove temporary files generated during the execution of the test or to returnsetting to their previous or more secure values so that the test can be run again. Running the cleanup commands after every test execution is recommended.

1. To cleanup for a specific test

```
Invoke-AtomicTest T1089 -TestNames "Uninstall Sysmon" -Cleanup
```

2. Cleanup for all the atomic tests

```
Invoke-AtomicTest T1089 -Cleanup
```

NOTE: To know what is happing behind the scenes, use "ShowDetails" for a specific technique and you will find the cleanup command that will be executed if we ran the above cleanup commands.

References:

- https://github.com/redcanaryco/invoke-atomicredteam
- https://github.com/redcanaryco/atomic-red-team
- https://atomicredteam.io/
- https://redcanary.com/atomic-red-team/