

Installing Atomic Red Team on Windows

Prerequisites:

- Windows operating system
- Powershell (preinstalled in Windows)

Step 1: Open google.com and search for the AtomicRedTeam GitHub page.

- Use the following link: <https://github.com/redcanaryco/invoke-atomicredteam/wiki>

The screenshot shows a web browser window displaying the GitHub Wiki page for the 'redcanaryco/invoke-atomicredteam' repository. The browser's address bar shows the URL 'https://github.com/redcanaryco/invoke-atomicredteam/wiki'. The page title is 'Home', and it notes that 'Carrie Roberts edited this page on Oct 16, 2020 · 19 revisions'. The main content area describes 'Invoke-AtomicRedTeam' as a PowerShell module for executing tests defined in the 'atomics' folder of the Red Canary's Atomic Red Team project. It mentions that each technique in the MITRE ATT&CK™ Framework has a corresponding 'T#' folder containing a 'yaml' file and a markdown version. A list of instructions follows: executing tests may leave the system in an undesirable state, ensuring permission to test, and setting up a test machine. It also provides links to installation and use instructions, a series of instructional videos on YouTube, and an in-depth 2-hour webcast. A sidebar on the right lists 13 pages, with 'Installation' as the first item. Below the sidebar, there is a 'Clone this wiki locally' section with a button to copy the URL 'https://github.com/redcanaryco/inv'. At the bottom of the page, there is a link to the 'Atomic Red Team Slack channel' for questions. The Windows taskbar is visible at the bottom of the screen, showing the search bar and several application icons.

Home · redcanaryco/invoke-atomicredteam Wiki · GitHub

Home

Carrie Roberts edited this page on Oct 16, 2020 · 19 revisions

Invoke-AtomicRedTeam is a PowerShell module to execute tests as defined in the [atomics folder](#) of Red Canary's Atomic Red Team project. The "atomics folder" contains a folder for each Technique defined in the MITRE ATT&CK™ Framework. Inside of each of these "T#" folders you'll find a **yaml** file that defines the attack procedures for each atomic test as well as an easier to read markdown (**md**) version of the same data.

- Executing atomic tests may leave your system in an undesirable state. You are responsible for understanding what a test does before executing.
- Ensure you have permission to test before you begin.
- It is recommended to set up a test machine for atomic test execution that is similar to the build in your environment. Be sure you have your collection/EDR solution in place, and that the endpoint is checking in and active.

Invoke-AtomicRedTeam installation and use instructions can be found on the index to the right (in the sidebar).

There are a series of short instructional videos on [this YouTube channel](#).

You can also find an in-depth 2 hour webcast [here](#).

Questions? Get connected to the community on the [Atomic Red Team Slack channel](#).

Pages 13

- Installation
- Import the Module
- List Atomic Tests
- Check/Get Prerequisites for Atomic Tests
- Execute Atomic Tests (Local)
- Execute Atomic Tests (Remote)
- Specify Custom Input Arguments
- Cleanup after Executing Atomic Tests
- Helper Functions
- The Atomic GUI

Clone this wiki locally

<https://github.com/redcanaryco/inv>

Step 2: Click "Installation" on the right side.

Red
d in
nes the
me

► Pages **13**

- **Installation**
- Import the Module
- List Atomic Tests
- Check/Get Prerequisites for Atomic Tests
- Execute Atomic Tests (Local)
- Execute Atomic Tests (Remote)
- Specify Custom Input Arguments
- Cleanup after Executing Atomic Tests
- Helper Functions
- The Atomic GUI

in
it is

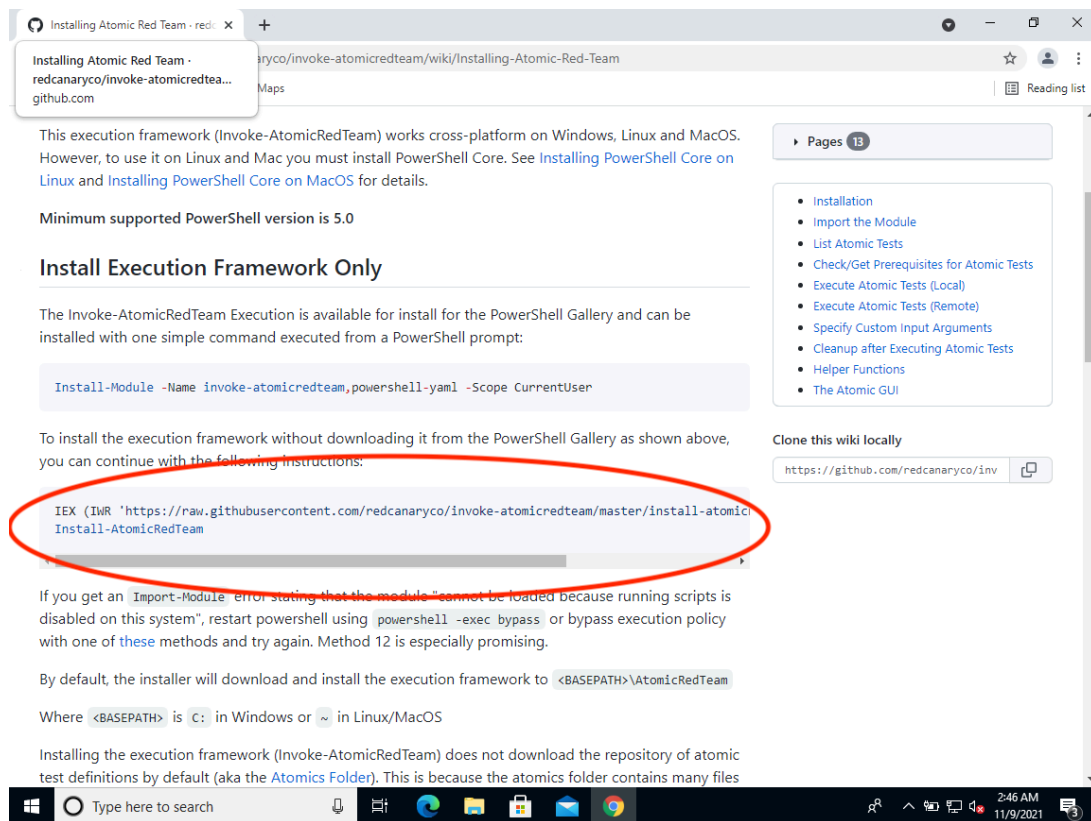
he

Clone this wiki locally

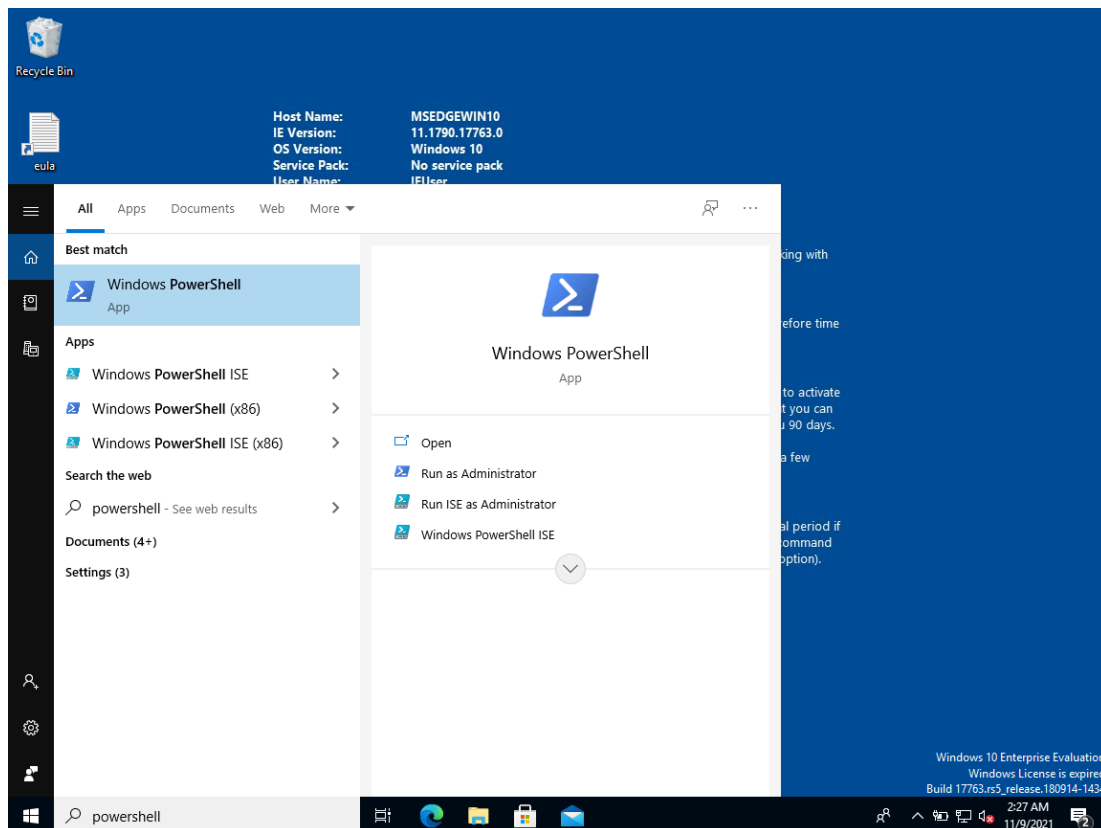
<https://github.com/redcanaryco/inv>



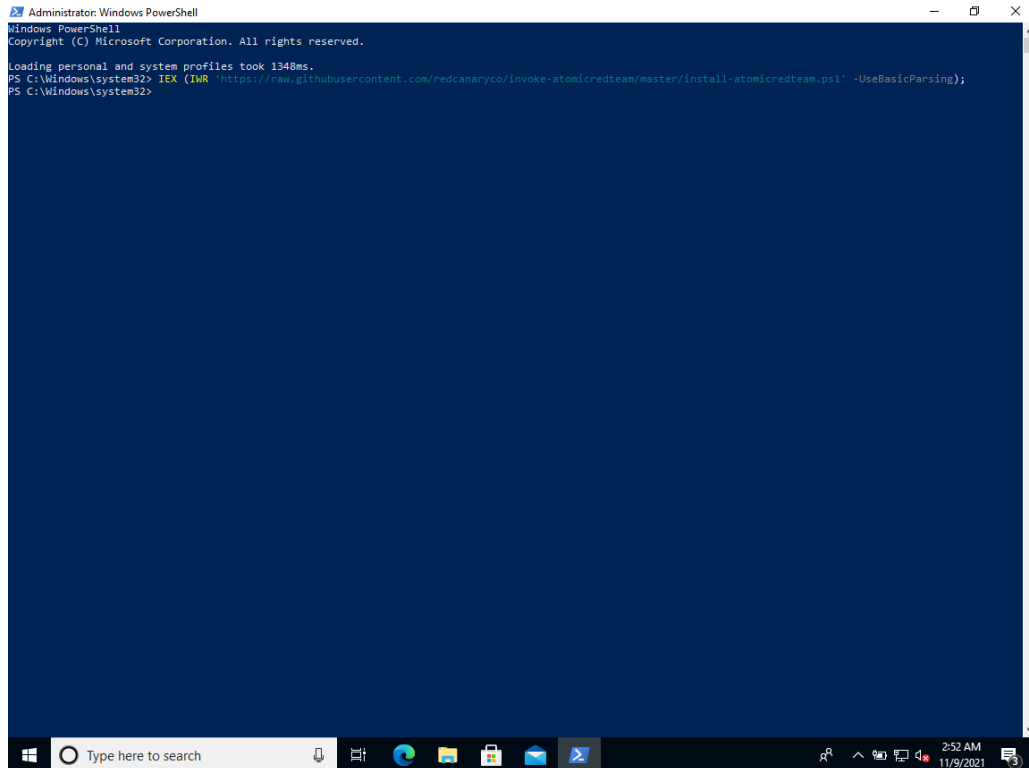
Step 3: Copy the link under “install execution framework only”



Step 4: Open Powershell and run it as Administrator.



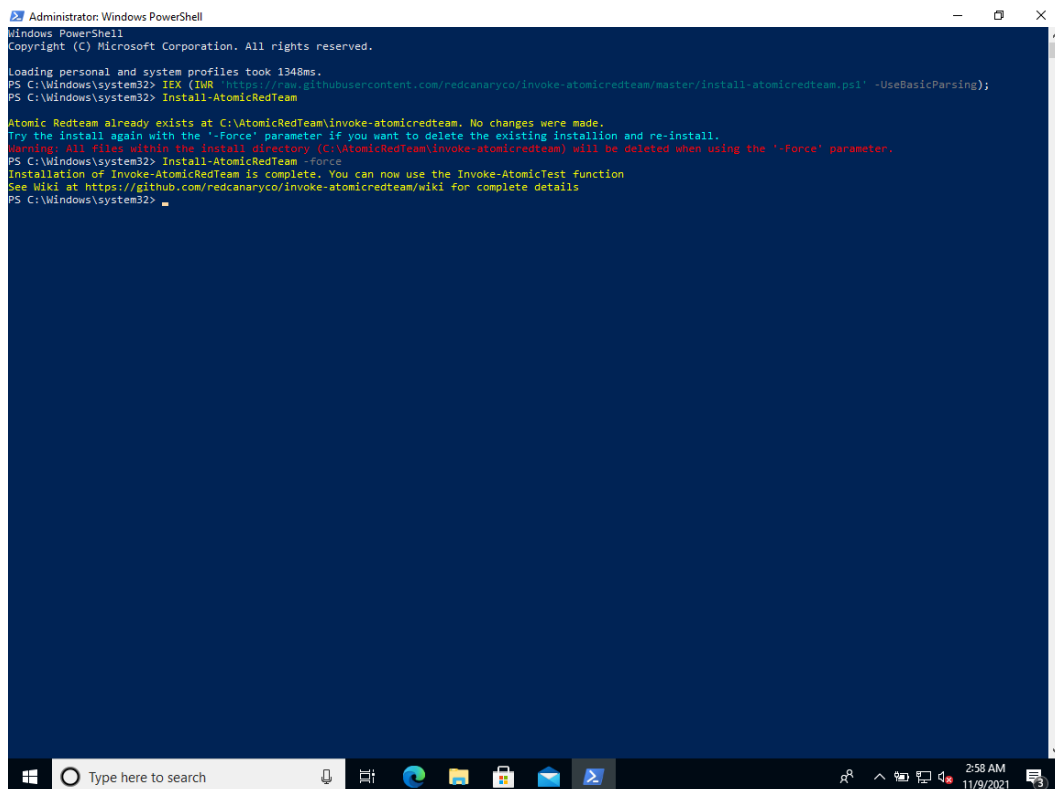
Step 5: Paste the copied command and run it.



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Loading personal and system profiles took 1348ms.
PS C:\Windows\system32> IEX (IWR 'https://raw.githubusercontent.com/redcanaryco/atomicredteam/master/install-atomicredteam.ps1' -UseBasicParsing);
PS C:\Windows\system32>
```

Step 6: Run “Install-AtomicRedTeam” and after installing it should say “Installation of atomic red team is complete”
(In my case it is already installed so it'll pop out some error or it'll tell me to use the “-force” command)



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Loading personal and system profiles took 1348ms.
PS C:\Windows\system32> IEX (IWR 'https://raw.githubusercontent.com/redcanaryco/atomicredteam/master/install-atomicredteam.ps1' -UseBasicParsing);
PS C:\Windows\system32> Install-AtomicRedTeam

Atomic Redteam already exists at C:\AtomicRedTeam\invoke-atomicredteam. No changes were made.
Try the install again with the '-Force' parameter if you want to delete the existing installation and re-install.
Warning: All files within the Atomic directory (C:\AtomicRedTeam\invoke-atomicredteam) will be deleted when using the '-Force' parameter.
PS C:\Windows\system32> Install-AtomicRedTeam -force
Installation of Invoke-AtomicRedTeam is complete. You can now use the Invoke-AtomicTest function
See Wiki at https://github.com/redcanaryco/atomicredteam/wiki for complete details
PS C:\Windows\system32>
```

Step 7: Run “Invoke-AtomicRedTeam -getatomics” After installation it should say “Installation of Invoke-AtomicRedTeam is complete”.

```
Administrator: Windows PowerShell
PS C:\Windows\system32> Install-AtomicRedTeam -getatomics
Atomic Redteam already exists at C:\AtomicRedTeam\invoke-atomicredteam. No changes were made.
Try the install again with the '-Force' parameter if you want to delete the existing installation and re-install.
Warning: All files within the install directory (C:\AtomicRedTeam\invoke-atomicredteam) will be deleted when using the '-Force' parameter.
PS C:\Windows\system32> Install-AtomicRedTeam -getatomics -force
Access to the path 'AtomicService.exe' is denied.
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>
```

Step 8: To cross-check whether you've installed it correctly, open File Explorer and go to C:\AtomicRedTeam\atomics there you'll find all the atomic tests. Hence you've installed Atomic Red Team on Windows

