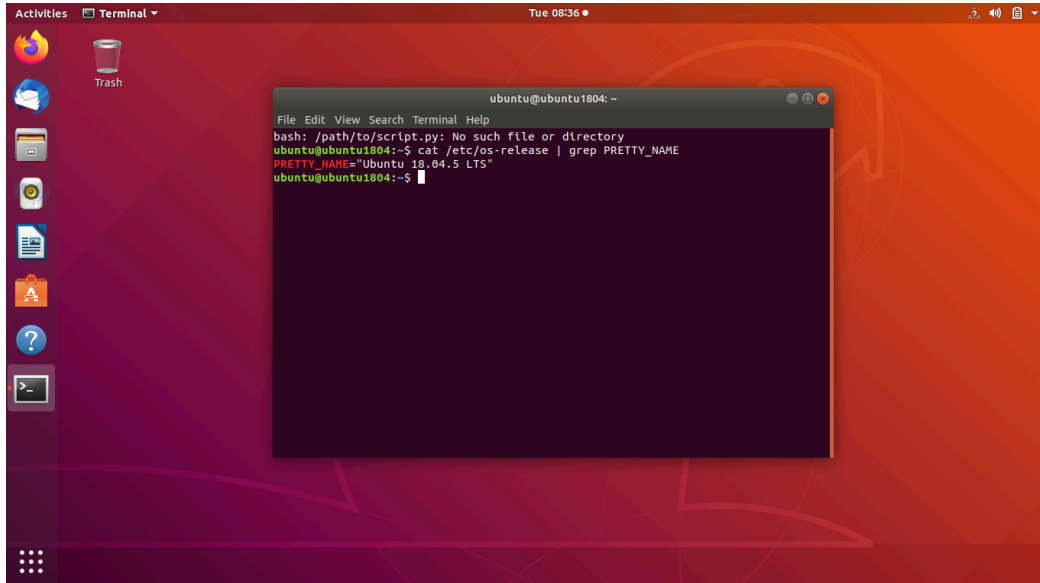


# Installing Atomic Red Team in Linux

## Prerequisites:

- Linux OS (UBUNTU - my preference)
- Powershell Core

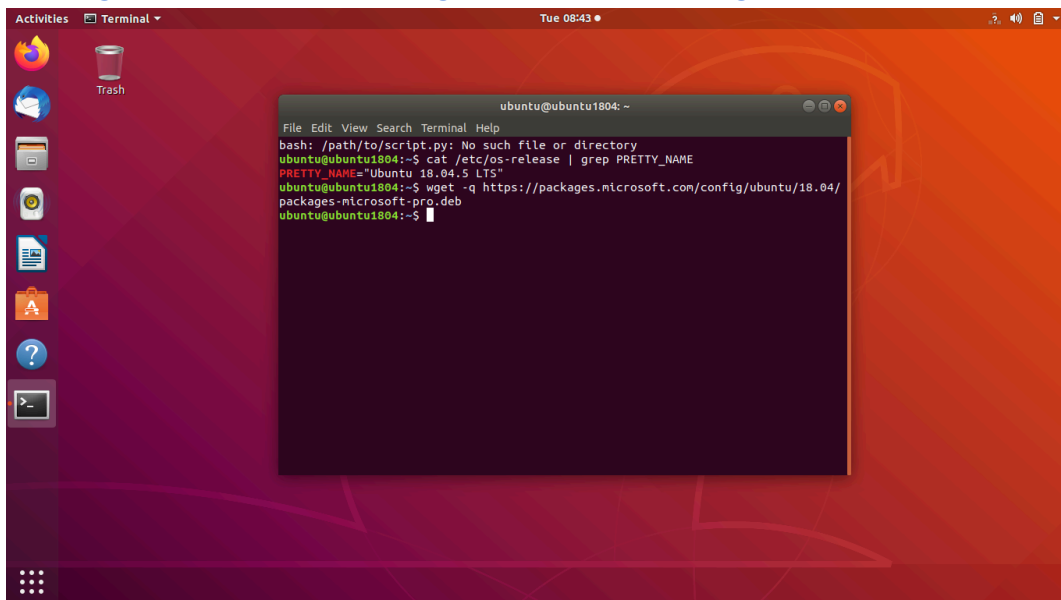
Step 1: Open Ubuntu and check the version of your OS using the command “cat /etc/os-release | grep PRETTY\_NAME”



```
ubuntu@ubuntu1804: ~  
File Edit View Search Terminal Help  
bash: /path/to/script.py: No such file or directory  
ubuntu@ubuntu1804:~$ cat /etc/os-release | grep PRETTY_NAME  
PRETTY_NAME="Ubuntu 18.04.5 LTS"  
ubuntu@ubuntu1804:~$
```

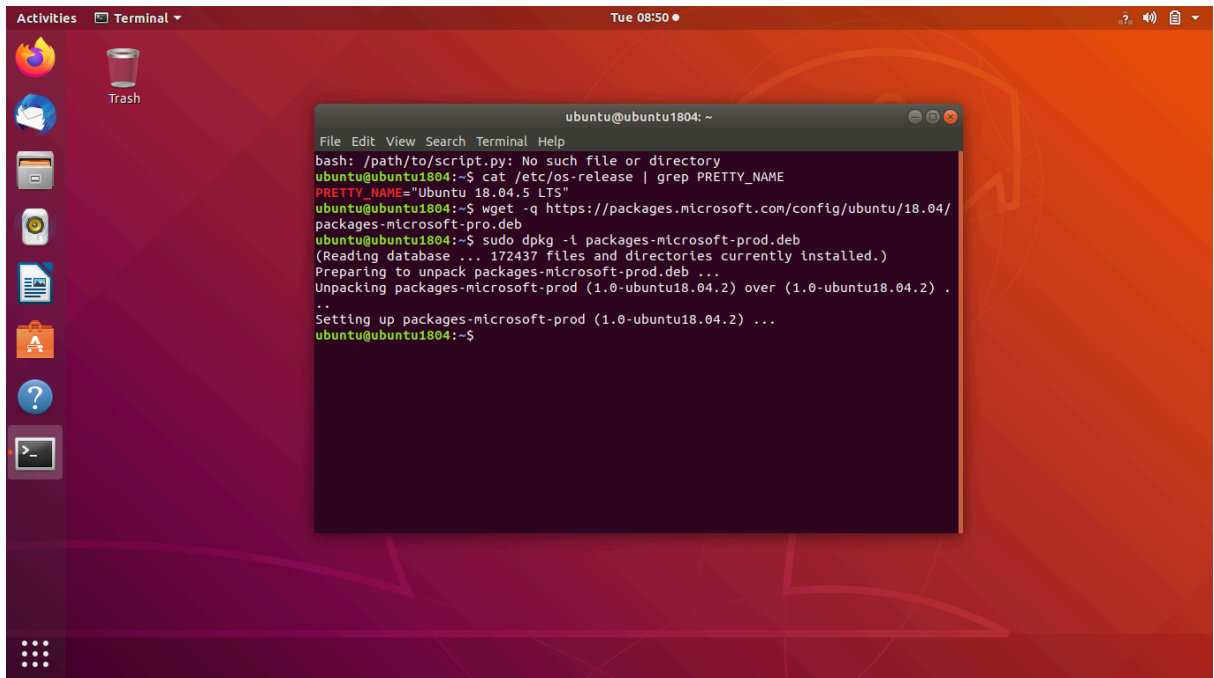
Step 2: now download the Microsoft repositories that are specific to this release using the command “wget -q

<https://packages.microsoft.com/config/ubuntu/18.04/packages-microsoft-prod.deb>”



```
ubuntu@ubuntu1804: ~  
File Edit View Search Terminal Help  
bash: /path/to/script.py: No such file or directory  
ubuntu@ubuntu1804:~$ cat /etc/os-release | grep PRETTY_NAME  
PRETTY_NAME="Ubuntu 18.04.5 LTS"  
ubuntu@ubuntu1804:~$ wget -q https://packages.microsoft.com/config/ubuntu/18.04/packages-microsoft-prod.deb  
ubuntu@ubuntu1804:~$
```

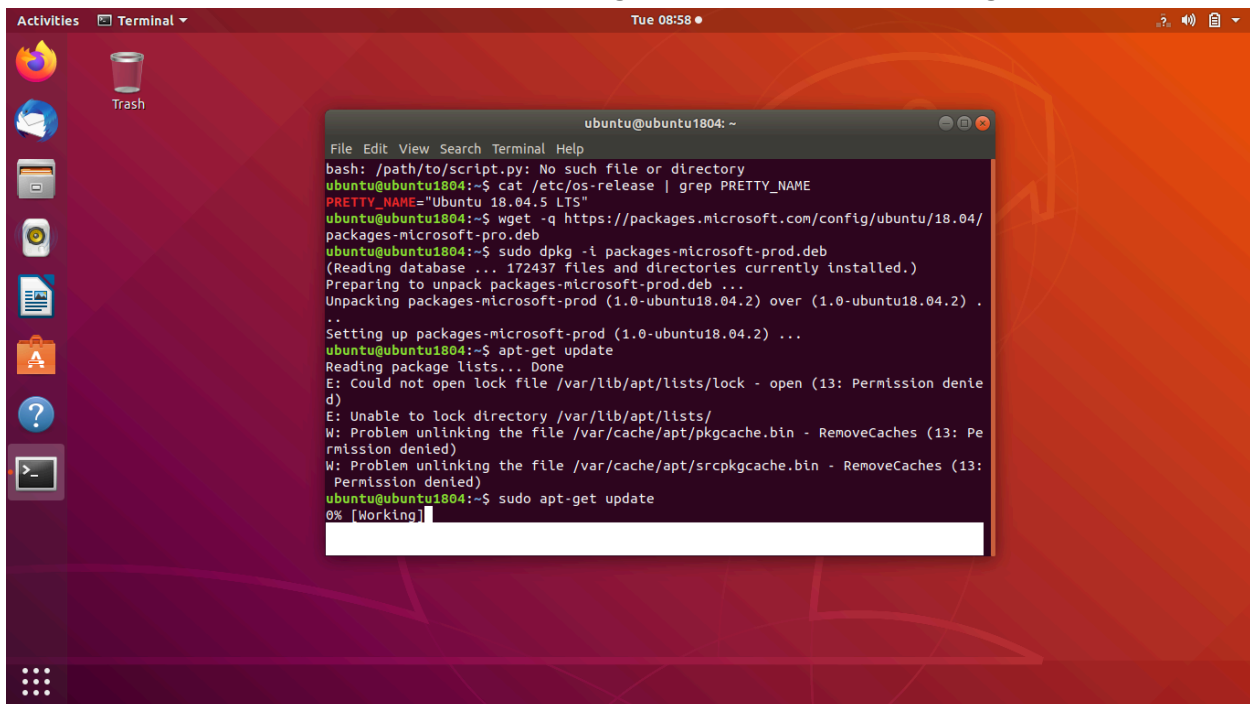
Step 3: now register the downloaded dpkg using the command “sudo dpkg -i packages-microsoft-prod.deb”



The terminal window shows the following commands and output:

```
ubuntu@ubuntu1804: ~  
File Edit View Search Terminal Help  
bash: /path/to/script.py: No such file or directory  
ubuntu@ubuntu1804:~$ cat /etc/os-release | grep PRETTY_NAME  
PRETTY_NAME="Ubuntu 18.04.5 LTS"  
ubuntu@ubuntu1804:~$ wget -q https://packages.microsoft.com/config/ubuntu/18.04/packages-microsoft-prod.deb  
ubuntu@ubuntu1804:~$ sudo dpkg -i packages-microsoft-prod.deb  
(Reading database ... 172437 files and directories currently installed.)  
Preparing to unpack packages-microsoft-prod.deb ...  
Unpacking packages-microsoft-prod (1.0-ubuntu18.04.2) over (1.0-ubuntu18.04.2) ...  
Setting up packages-microsoft-prod (1.0-ubuntu18.04.2) ...  
ubuntu@ubuntu1804:~$
```

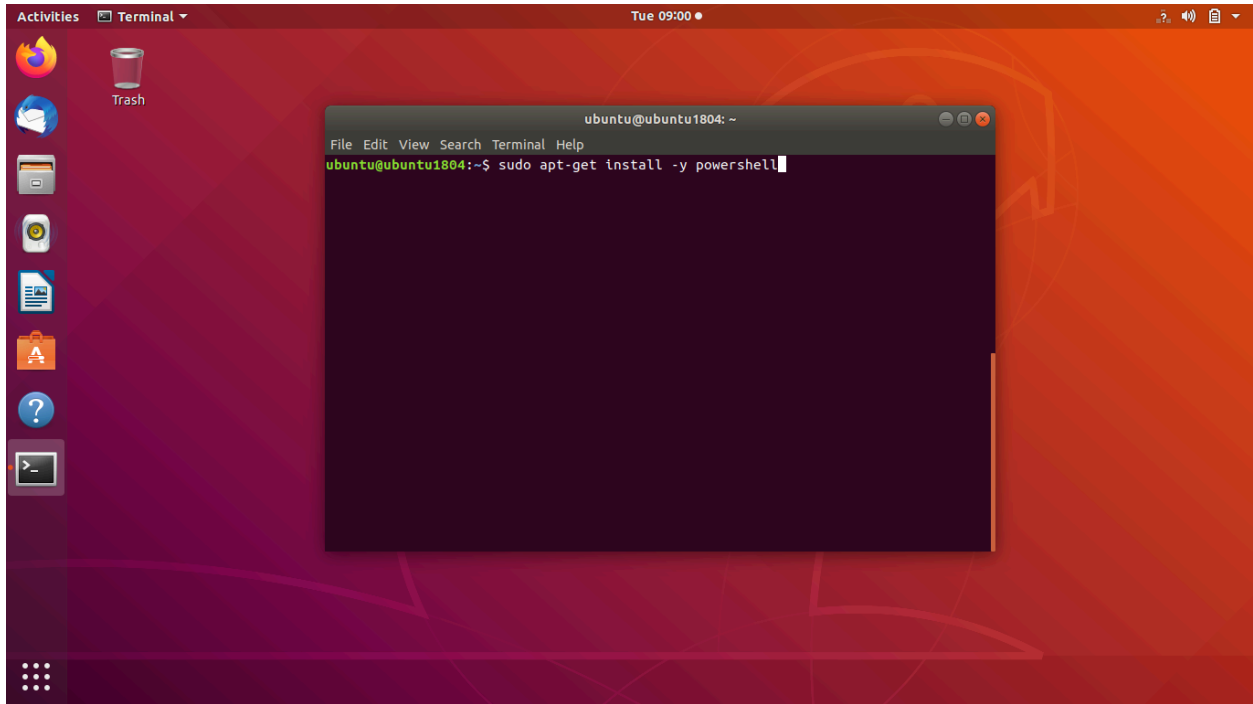
**Step 4: now update the list of products using the command “sudo apt-get update”**



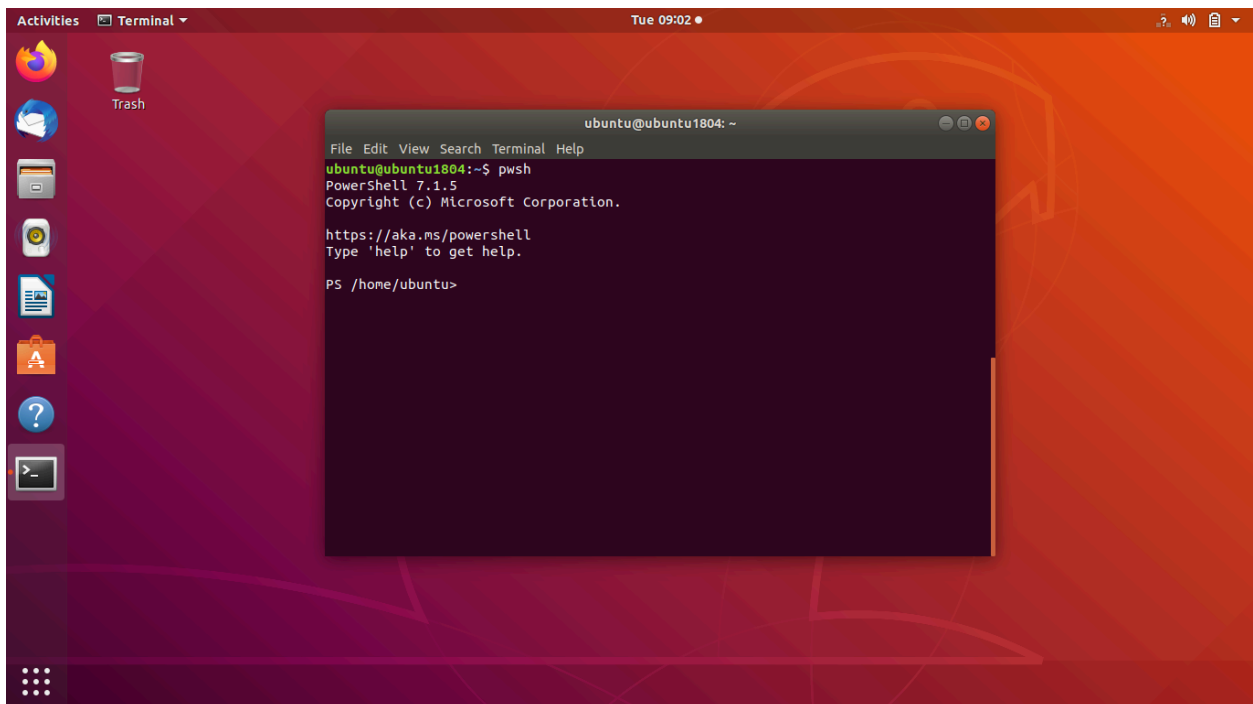
The terminal window shows the following commands and output:

```
ubuntu@ubuntu1804: ~  
File Edit View Search Terminal Help  
bash: /path/to/script.py: No such file or directory  
ubuntu@ubuntu1804:~$ cat /etc/os-release | grep PRETTY_NAME  
PRETTY_NAME="Ubuntu 18.04.5 LTS"  
ubuntu@ubuntu1804:~$ wget -q https://packages.microsoft.com/config/ubuntu/18.04/packages-microsoft-prod.deb  
ubuntu@ubuntu1804:~$ sudo dpkg -i packages-microsoft-prod.deb  
(Reading database ... 172437 files and directories currently installed.)  
Preparing to unpack packages-microsoft-prod.deb ...  
Unpacking packages-microsoft-prod (1.0-ubuntu18.04.2) over (1.0-ubuntu18.04.2) ...  
Setting up packages-microsoft-prod (1.0-ubuntu18.04.2) ...  
ubuntu@ubuntu1804:~$ apt-get update  
Reading package lists... Done  
E: Could not open lock file /var/lib/apt/lists/lock - open (13: Permission denied)  
E: Unable to lock directory /var/lib/apt/lists/  
W: Problem unlinking the file /var/cache/apt/pkgcache.bin - RemoveCaches (13: Permission denied)  
W: Problem unlinking the file /var/cache/apt/srcpkgcache.bin - RemoveCaches (13: Permission denied)  
ubuntu@ubuntu1804:~$ sudo apt-get update  
0% Working
```

**Step 5: Now install the PowerShell core using the command “sudo apt-get install -y powershell”**



**Step 6: After installing the PowerShell invoke the PowerShell by using the command “pwsh”**



Hence Powershell Core is installed on our linux machine and now we've to install atomic Red Team in our linux using Powershell. It follows the same steps from now on as we follow in the installation of the atomic red team in Windows.

**Step 7: Go to the Atomic Red Team GitHub page where the installation command is available.**

<https://github.com/redcanaryco/invoke-atomicredteam/wiki/Installing-Atomic-Red-Team>

The screenshot shows a web browser window displaying the GitHub Wiki page for 'Installing Atomic Red Team' by redcanaryco. The page is titled 'Installing Atomic Red Team' and mentions that it was last edited by Carrie Roberts on August 19, 2019. The page content includes instructions for installing the execution framework, with a minimum supported PowerShell version of 5.0. It provides a PowerShell command to install the module and explains how to handle errors related to script execution. The page also covers installing the 'Atomics Folder' and provides optional installation parameters like 'InstallPath' and 'Force'. A sidebar on the right lists various pages related to the framework, such as 'Installation', 'Import the Module', and 'Execute Atomic Tests'. The browser's address bar shows the URL 'https://github.com/redcanaryco/invoke-atomicredteam/wiki/Installing-Atomic-Red-Team'.

## Installing Atomic Red Team

Carrie Roberts edited this page on Aug 19 · 36 revisions

This execution framework (Invoke-AtomicRedTeam) works cross-platform on Windows, Linux and MacOS. However, to use it on Linux and Mac you must install PowerShell Core. See [Installing PowerShell Core on Linux](#) and [Installing PowerShell Core on MacOS](#) for details.

**Minimum supported PowerShell version is 5.0**

### Install Execution Framework Only

The Invoke-AtomicRedTeam Execution is available for install for the PowerShell Gallery and can be installed with one simple command executed from a PowerShell prompt:

```
Install-Module -Name invoke-atomicredteam, powershell-yaml -Scope CurrentUser
```

To install the execution framework without downloading it from the PowerShell Gallery as shown above, you can continue with the following instructions:

```
EX (IWR 'https://raw.githubusercontent.com/redcanaryco/invoke-atomicredteam/master/install-atomicredteam' -Uri) Install-AtomicRedTeam
```

If you get an 'Import-Module' error stating that the module "cannot be loaded because running scripts is disabled on this system", restart powershell using 'powershell -exec bypass' or bypass execution policy with one of [these](#) methods and try again. Method 12 is especially promising.

By default, the installer will download and install the execution framework to <BASEPATH>\AtomicRedTeam

Where <BASEPATH> is C: in Windows or / in Linux/MacOS

Installing the execution framework (Invoke-AtomicRedTeam) does not download the repository of atomic test definitions by default (aka the **Atomics Folder**). This is because the atomics folder contains many files likely to trigger AV alerts on the endpoint. You may choose to white-list the install directory (<BASEPATH>\AtomicRedTeam by default) so that files are not quarantined or removed. Or you may choose to copy a version of the atomics folder over to the system that contains only the tests you intend to run.

### Install Execution Framework and Atomics Folder

The **Atomics Folder** contains the test definitions; the commands that the execution framework will execute. If you would like to install the atomics folder at the same time that you install the execution framework, you can do this by adding the -getAtomics switch during the install of the execution framework.

```
EX (IWR 'https://raw.githubusercontent.com/redcanaryco/invoke-atomicredteam/master/install-atomicredteam' -Uri) Install-AtomicRedTeam -getAtomics
```

If the execution framework or the atomics folder are already found on disk you must use the -Force parameter during install as follows to erase and replace these folders.

```
EX (IWR 'https://raw.githubusercontent.com/redcanaryco/invoke-atomicredteam/master/install-atomicredteam' -Uri) Install-AtomicRedTeam -getAtomics -Force
```

### Install Atomics Folder Only

If you would like to install the atomics folder as a separate step or at a later time, you can do it with the **Install-AtomicsFolder** function as follows.

```
EX (IWR 'https://raw.githubusercontent.com/redcanaryco/invoke-atomicredteam/master/install-atomicsfolder' -Uri) Install-AtomicsFolder
```

### Optional Installation Parameters

Both the Install-AtomicRedTeam and the Install-AtomicsFolder functions have the following optional parameters:

**InstallPath**

- Where to install (default: C:\AtomicRedTeam on Windows or ~/AtomicRedteam on MacOS and Linux)

```
Install-AtomicRedTeam -InstallPath "c:\tools"
Install-AtomicsFolder -InstallPath "c:\tools"
```

**Force**

- Remove the previous installation before installing

**Step 8: copy the command, and run it in Powershell.**

Activities Firefox Web Browser Tue 10:23

Installing Atomic Red Team - redcanaryco/Invoke-atomicredteam Wiki - GitHub - Mozilla Firefox

Index of /config/ubuntu/18: X Installing Atomic Red Team X

https://github.com/redcanaryco/Invoke-atomicredteam/wiki/Installing-Atomic-Red-Team

Why GitHub? Team Enterprise Explore Marketplace Pricing

Search Sign in Sign up

redcanaryco / Invoke-atomicredteam Public

Notifications Star 303 Fork 100

Code Issues 11 Pull requests 1 Wiki Security Insights

## Installing Atomic Red Team

Carrie Roberts edited this page on Aug 19 · 36 revisions

This execution framework (Invoke-AtomicRedTeam) works cross-platform on Windows, Linux and MacOS. However, to use it on Linux and Mac you must install PowerShell Core. See [Installing PowerShell Core on Linux](#) and [Installing PowerShell Core on MacOS](#) for details.

Minimum supported PowerShell version is 5.0

### Install Execution Framework Only

The Invoke-AtomicRedTeam Execution is available for install for the PowerShell Gallery and can be installed with one simple command executed from a PowerShell prompt:

```
Install-Module -Name Invoke-atomicredteam,powershell-yaml -Scope CurrentUser
```

To install the execution framework without downloading it from the PowerShell Gallery as shown above, you can continue with the following instructions:

```
IEX (IWR 'https://raw.githubusercontent.com/redcanaryco/Invoke-atomicredteam/master/Install-atomicredteam
Install-AtomicRedTeam
```

If you get an `Import-Module` error stating that the module "cannot be loaded because running scripts is disabled on this system", restart powershell using `powershell -exec bypass` or bypass execution policy with one of [these](#) methods and try again. Method 12 is especially promising.

By default, the installer will download and install the execution framework to `<BASEPATH>\AtomicRedTeam`

Where `<BASEPATH>` is `C:` in Windows or `~` in Linux/MacOS

Installing the execution framework (Invoke-AtomicRedTeam) does not download the repository of atomic test definitions by default (aka the [Atomics Folder](#)). This is because the atomics folder contains many files likely to trigger AV alerts on the endpoint. You may choose to white-list the install directory (`<BASEPATH>\AtomicRedTeam` by default) so that files are not quarantined or removed. Or you may choose to copy a version of the atomics folder over to the system that contains only the tests you intend to run.

### Install Execution Framework and Atomics Folder

The [Atomics Folder](#) contains the test definitions; the commands that the execution framework will execute. If you would like to install the atomics folder at the same time that you install the execution framework, you can do this by adding the `-getAtomics` switch during the installation:

```
IEX (IWR 'https://raw.githubusercontent.com/redcanaryco/Invoke-atomicredteam/master/Install-atomicredteam
Install-AtomicRedTeam -getAtomics
```

If the execution framework or the atomics folder are already installed, you must use the `-Force` parameter during install as follows to erase and replace these folders.

```
IEX (IWR 'https://raw.githubusercontent.com/redcanaryco/Invoke-atomicredteam/master/Install-atomicredteam
Install-AtomicRedTeam -getAtomics -Force
```

### Install Atomics Folder Only

If you would like to install the atomics folder as a separate step or at a later time, you can do it with the `Install-AtomicsFolder` function as follows.

```
IEX (IWR 'https://raw.githubusercontent.com/redcanaryco/Invoke-atomicredteam/master/Install-atomicsFolder
Install-AtomicsFolder
```

### Optional Installation Parameters

Both the `Install-AtomicRedTeam` and the `Install-AtomicsFolder` functions have the following optional parameters:

**InstallPath**

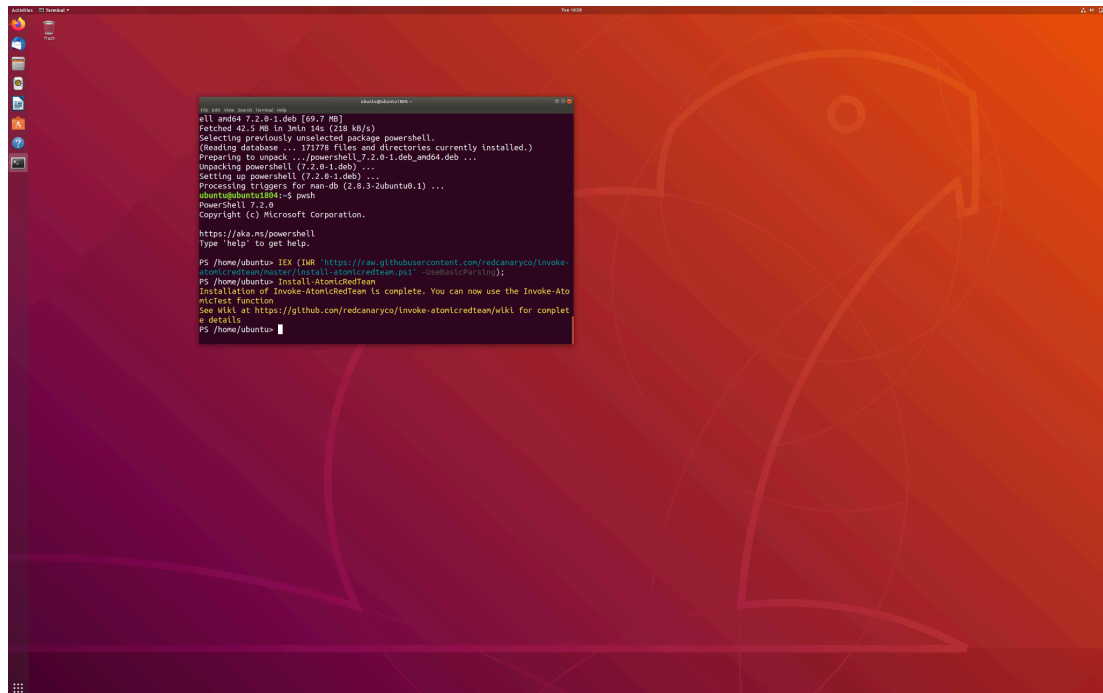
- Where to install (default: `C:\AtomicRedTeam` on Windows or `~\AtomicRedteam` on MacOS and Linux)

```
Install-AtomicRedTeam -InstallPath "c:\tools"
Install-AtomicsFolder -InstallPath "c:\tools"
```

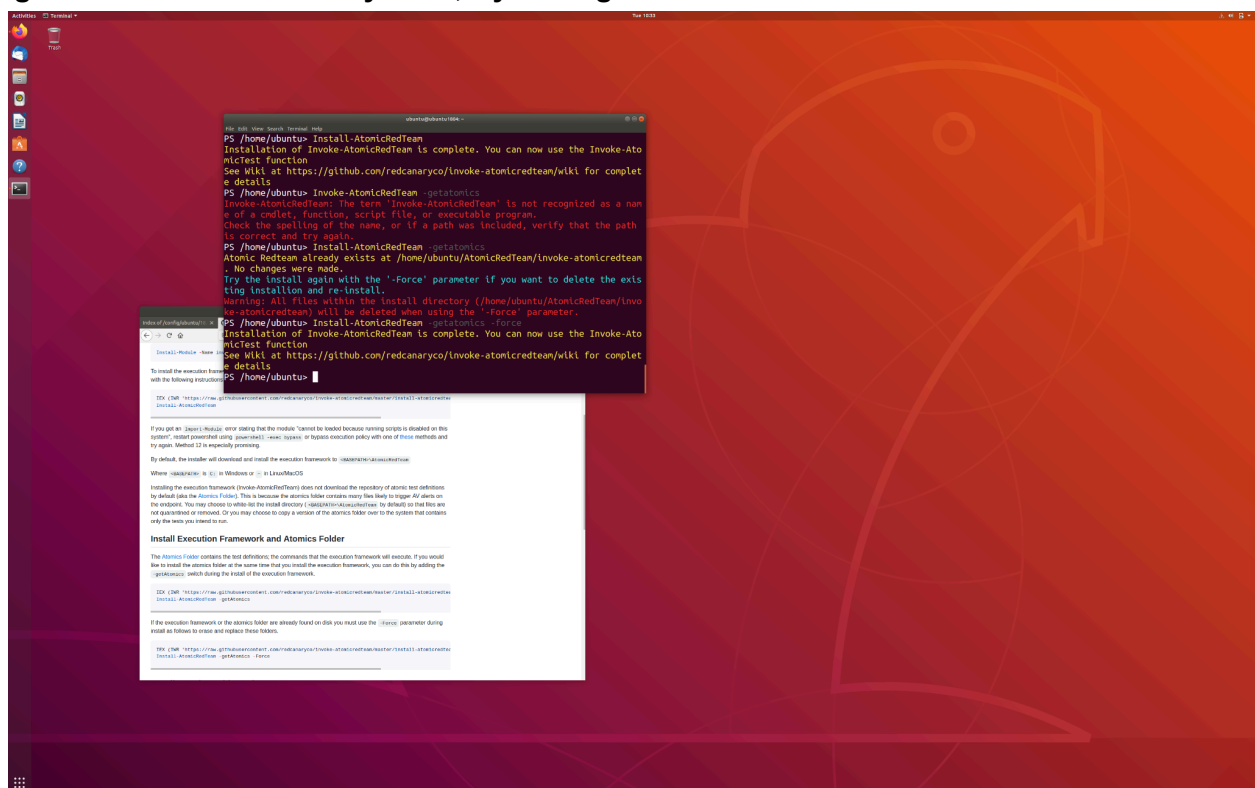
**Force**

- Remove the previous installation before installing

**Step 9: After installation, it should tell you that "Invoke-AtomicRedTeam is complete".**



**Step 10: then install the atomics folder by using the command “Install-AtomicRedTeam -getatomics” If there is any error, try adding “-force” at the end of the command.**



**Now You're ready with your Atomic Red Team in linux. Use Invoke-AtomicTest <Test numbers> syntax to run your atomic tests.**

