

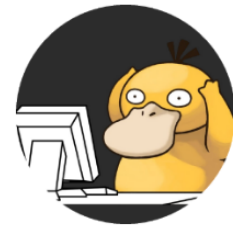
hausec/PowerZure: PowerShell framework to assess Azure security

 github.com/hausec/PowerZure

hausec


hausec/PowerZure

PowerShell framework to assess Azure security

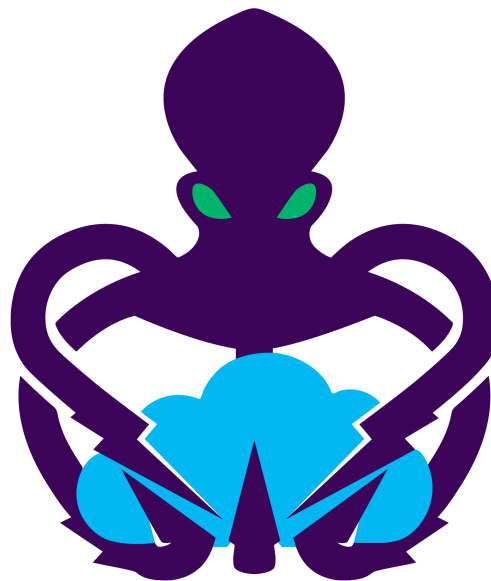


 3
Contributors

 0
Issues

 721
Stars

 122
Forks



PowerZure

For a list of functions, their usage, and more, check out <https://powerzure.readthedocs.io>

What is PowerZure?

PowerZure is a PowerShell project created to assess and exploit resources within Microsoft's cloud platform, Azure. PowerZure was created out of the need for a framework that can both perform reconnaissance **and** exploitation of Azure, AzureAD, and the associated resources.

Requirements

The "Az" Azure PowerShell module is the primary module used in PowerZure, as it handles most requests interacting with Azure resources. The Az module interacts using the Azure REST API. It can be installed via PowerShell command `Install-Module -Name Az`

The AzureAD PowerShell Module is also used and is for handling AzureAD requests. The AzureAD module uses the Microsoft Graph API and can be installed via the PowerShell command `Install-Module -Name AzureAD`

Usage

RTFM: <https://powerzure.readthedocs.io>

```
ipmo C:\path\to\PowerZure.psd1
```

If you have multiple subscriptions, you must set the main subscription with `Set-AzureSubscription`. If you do not do this, things will fail.

Additional Resources

You can type `Show-AzureCurrentUser` to view the current signed-in user's roles in Azure and Azure AD.

You can also type `Get-AzureTargets` to compare your current signed-in user's roles and their scope to resources within Azure.

For target finding, I recommend using AzureHound, the Azure component to BloodHound.

Author & License

Author: Ryan Hausknecht (@haus3c)

License: BSD-3