Security Auditing

- ScoutSuite
- PowerZure
- Get help for a particular function
- Get all content from all KeyVault
- MicroBurst
- SkyArk

ScoutSuite

https://github.com/nccgroup/ScoutSuite will generate an HTML report outlining various issues that exist in the configuration for a given account.

Install:

```
git clone git@github.com:nccgroup/ScoutSuite.git
cd ScoutSuite
pipenv --python 3
pipenv shell
pip install -r requirements.txt
```

Run:

```
python scout.py azure --cli
```

Resources: https://kalilinuxtutorials.com/scout-suite-multi-cloud-security-auditing-tool/

PowerZure

```
git clone git@github.com:hausec/PowerZure.git
cd PowerZure
pwsh-preview

# Authenticate
Connect-AzAccount

# Import PowerZure
# impo is shorthand for Import-Module
ipmo ./PowerZure.ps1

# If you have multiple subscriptions, set the one you want to target:
Set-AzureSubscription -Id [Subscription ID]

# Enumerate all roles
Get-AzureRole

# Enumerate resources the current user has access to
Get-AzureTargets

# Show info about current user
Show-AzureCurrentUser
```

Resources:

https://powerzure.readthedocs.io/en/latest/

Fix error when importing AzureADPreview

Fix missing modules

Show all functions

```
powerzure -h
```

Get help for a particular function

For example:

```
get-help Get-AzureTargets
```

Get all content from all KeyVault

```
Show-AzureKeyVaultContent -All
```

Resource:

https://hausec.com/2020/01/31/attacking-azure-azure-ad-and-introducing-powerzure/

MicroBurst

```
git clone git@github.com:NetSPI/MicroBurst.git
cd MicroBurst

pwsh-preview

# Authenticate
Connect-AzAccount

# Import MicroBurst
ipmo ./MicroBurst.psm1

# Install module for Out-GridView
Install-Module Microsoft.PowerShell.GraphicalTools

# Show commands
Get-Command -Module MicroBurst

# Dump info from an Azure subscription
**Note:** Be sure to click a row in the pop up before clicking **Export**
Get-AzDomainInfo -folder MicroBurst -Verbose

# Look for creds or certificate stores in a number of places and dump them to `secrets.txt`
**Note:** Be sure to click a row in the pop up before clicking **Export**
Get-AzPasswords -Verbose | Out-File -FilePath ./secrets.txt

# Dump Key Vault Keys and Secrets from an Azure subscription
# via Automation Accounts specifically
**Note:** Be sure to click a row in the pop up before clicking **Export**
Get-AzKeyVaultsAutomation -Verbose
```

Resources:

Where I found out about the tool initially

Write output to a file

SkyArk

```
git clone https://github.com/cyberark/SkyArk
cd SkyArk
pwsh-preview
Import-Module .\SkyArk.ps1 -force
Start-AzureStealth
```

Resource: https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology and Resources/Cloud - Azure Pentest.md