# PwnCloudOS

Welcome to PwnCloudOS! Brought to you by PwnedLabs, this platform is a treat for cloud security enthusiasts. PwnCloudOS is tailor-made to streamline your cloud Pentesting journey, eliminating the hassles of tool installations and dependency issues.

Picture having all the essential tools at your fingertips—be it PowerShell, Linux CLI, or Python applications—ready for immediate use. With PwnCloudOS, you can jump straight into PwnedLabs hands-on labs and bootcamp pathway challenges without the setup delays. We've even included a quick-start guide to get you up and running. Let's make your cloud security learning experience both smooth and enjoyable!

Login Page

- **Default Password:** `pwnedlabs`

Upon logging in, you will be welcomed by the main interface, ready to access the tools and utilities.
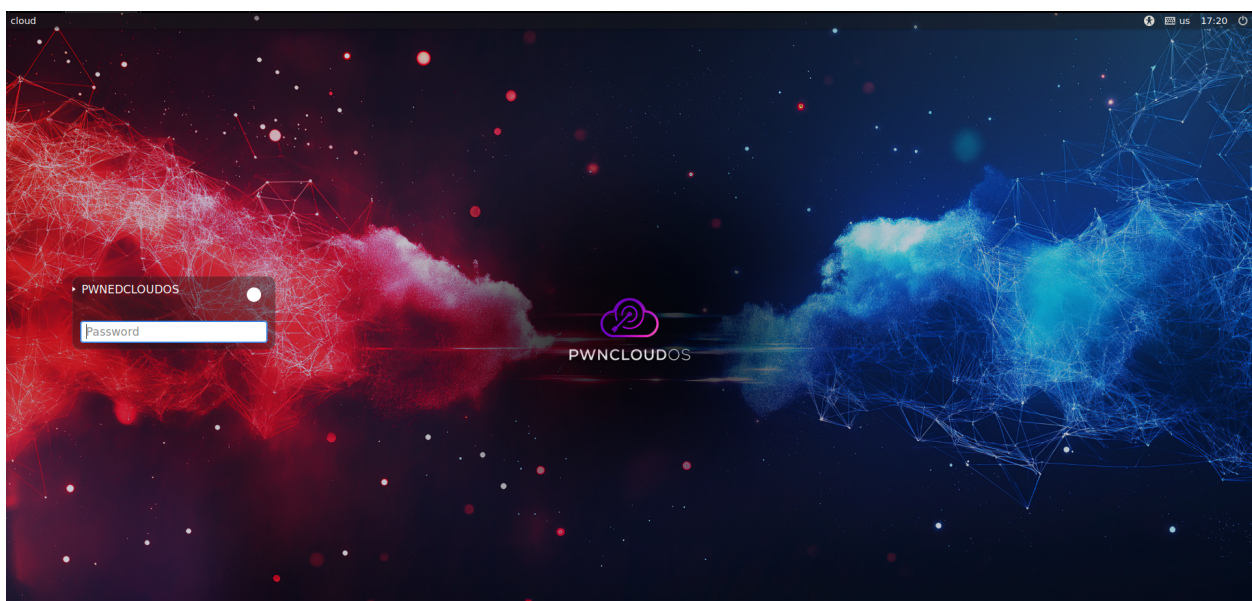
Main Interface

After logging in, you'll find a clean interface where all essential tools are organized in one-click launchers accessible through the **Menu.**

Accessing Tools via the Menu

To access your tools, click on the **Menu**. All tools are grouped into categories, each with its own launcher. For example:

- **MFASweep** - Opens PowerShell and provides instructions on importing and invoking the module, with step-by-step guidance.
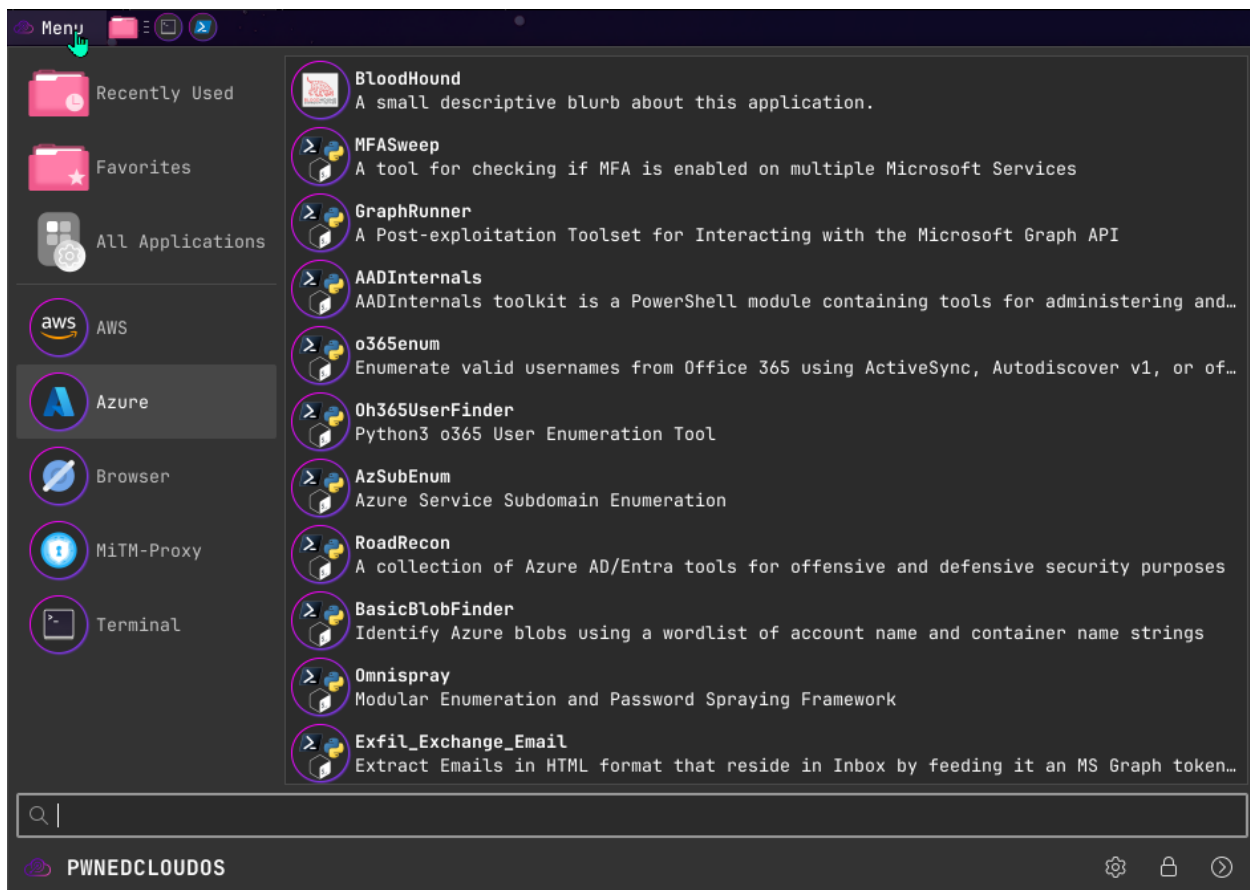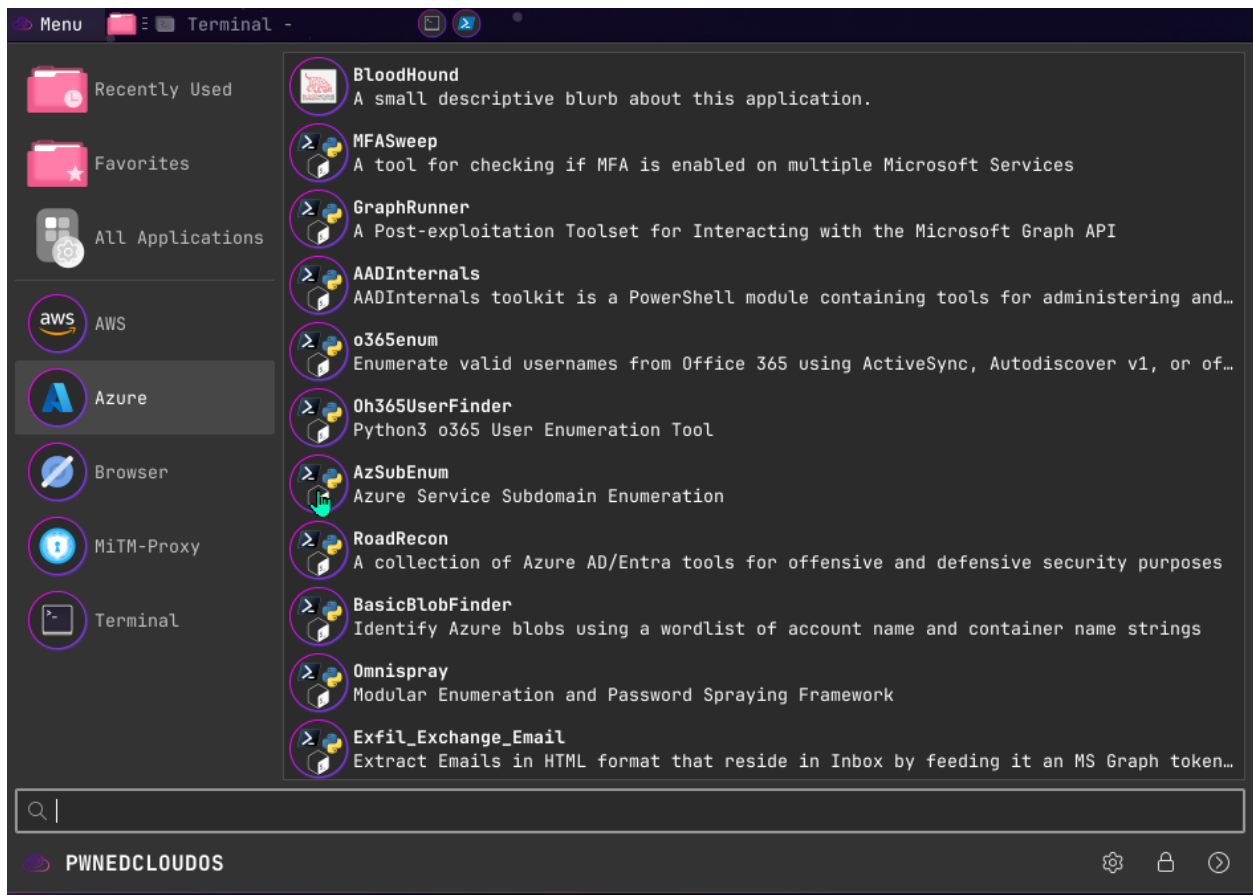
Python Tools - Clicking a Python tool like **AzSubEnum** navigates to the tool's folder location and provides a command example for usage.

BloodHound
A small descriptive blurb about this application.

MFASweep
A tool for checking if MFA is enabled on multiple Microsoft Services

GraphRunner
A Post-exploitation Toolset for Interacting with the Microsoft Graph API

AADInternals
AADInternals toolkit is a PowerShell module containing tools for administering and…

o365enum
Enumerate valid usernames from Office 365 using ActiveSync, Autodiscover v1, or of…

Oh365UserFinder
Python3 o365 User Enumeration Tool

AzSubEnum
Azure Service Subdomain Enumeration

RoadRecon
A collection of Azure AD/Entra tools for offensive and defensive security purposes

BasicBlobFinder
Identify Azure blobs using a wordlist of account name and container name strings

Omnispray
Modular Enumeration and Password Spraying Framework

Exfil_Exchange_Email
Extract Emails in HTML format that reside in Inbox by feeding it an MS Graph token…

Recently Used

Favorites

All Applications

AWS

Azure

Browser

MiTM-Proxy

Terminal

PWNEDCLOUDOS

```
     -p PERMUTATIONS, --permutations PERMUTATIONS
                         File containing permutations
     --blobsenum          Perform blob container enumeration
     -bw BW               Path to a custom wordlist file for blob container
                          enumeration
     -bt BT               Number of threads to use for blob container
                          enumeration

Examples:
Basic enumeration:

> python3 azsubenum.py -b retailcorp --thread 10
Using permutation wordlists:

> python3 azsubenum.py -b retailcorp --thread 10 --permutation permutations.txt
With verbose output:

> python3 azsubenum.py -b retailcorp --thread 10 --permutation permutations.txt
--verbose

For more information, visit: https://github.com/someone/AzSubEnum

┌─[pwnedlabs@cloud]─[/opt/azure_tools/AzSubEnum]
└─ $
```

```
┌─[pwnedlabs@cloud]─[/opt/azure_tools/AzSubEnum]
└─ $ ls
azsubenum_launcher.sh   permutations.txt   requirements.txt
azsubenum.py            README.md
```

Tool Directory Locations

All tools are organized by category, with specific directories for easy access:

- **AWS Tools**: `/opt/aws_tools`

- **Azure Tools**: `/opt/azure_tools`

- **PowerShell Tools**: `/opt/ps_tool`

You can access these locations directly or use the launchers to interact with each tool.

```
┌─[pwnedlabs@cloud]─[/opt]
└─ $ ls
aws_tools   azure_tools   burp   microsoft   ps_tools
```

```
┌─[pwnedlabs@cloud]─[/opt/azure_tools]
└─ $ ls
AzSubEnum      basicblobfinder   exfil_exchange_mail   o365spray        Omnispray
azure_hound    bloodhound        o365enum              0h365UserFinder  roadrecon
```

```
┌─[pwnedlabs@cloud]─[/opt/aws_tools]
└─ $ ls
pacu
```

```
┌─[pwnedlabs@cloud]─[/opt/ps_tools]
└─ $ ls
AADInternals   GraphRunner   invoke_modules   MFASweep   TokenTacticsV2
```