
MFASweep

MFASweep is a PowerShell script that attempts to log in to various Microsoft services using a provided set of credentials and will attempt to identify if MFA is enabled. Depending on how conditional access policies and other multi-factor authentication settings are configured some protocols may end up being left single factor. It also has an additional check for ADFS configurations and can attempt to log in to the on-prem ADFS server if detected.

Currently MFASweep has the ability to login to the following services:

- Microsoft Graph API
- Azure Service Management API
- Microsoft 365 Exchange Web Services
- Microsoft 365 Web Portal w/ 6 device types (Windows, Linux, MacOS, Android Phone, iPhone, Windows Phone)
- Microsoft 365 Active Sync
- ADFS

WARNING: This script attempts to login to the provided account TEN (10) different times (11 if you include ADFS). If you entered an incorrect password this may lock the account out.

For more information check out the blog post here: [Exploiting MFA Inconsistencies on Microsoft Services](#)

```

\Desktop> Invoke-MFASweep -Username smonkey@glitchcloud.com -Password 
----- MFASweep -----

Microsoft Services Recon
This script can attempt to determine if ADFS is configured for the domain you submitted. Would
you like to do this now?
[Y] Yes [N] No [?] Help (default is "Y"): y
----- Running recon checks -----
[*] Checking if ADFS configured...
[*] ADFS does not appear to be in use. Authentication appears to be managed by Microsoft.

Confirm MFA Sweep
[*] WARNING: This script is about to attempt logging into the smonkey@glitchcloud.com account
SIX (6) different times
(7 if you included ADFS). If you entered an incorrect password this may lock the account out.
Are you sure you want to
continue?
[Y] Yes [N] No [?] Help (default is "Y"): y

----- Microsoft Graph API -----
[*] Authenticating to Microsoft Graph API...
[*] SUCCESS! smonkey@glitchcloud.com was able to authenticate to the Microsoft Graph API - NOT
E: The response indicates MFA (Microsoft) is in use.

----- Azure Service Management API -----
[*] Authenticating to Azure Service Management API...
[*] SUCCESS! smonkey@glitchcloud.com was able to authenticate to the Azure Service Management
API - NOTE: The response indicates MFA (Microsoft) is in use.

----- Microsoft 365 Exchange Web Services -----
[*] Authenticating to Microsoft 365 Exchange Web Services (EWS)...
[*] SUCCESS! smonkey@glitchcloud.com was able to authenticate to Microsoft 365 EWS!
[***] NOTE: MailSniper should work here.

----- Microsoft 365 Web Portal -----
[*] Authenticating to Microsoft 365 Web Portal...
[*] SUCCESS! smonkey@glitchcloud.com was able to authenticate to the Microsoft 365 Web Portal.
Checking MFA now...
[**] It appears MFA is setup for this account to access Microsoft 365 via the web portal.

----- Microsoft 365 Web Portal w/ Mobile User Agent (Android) -----
[*] Authenticating to Microsoft 365 Web Portal using a mobile user agent...
[*] SUCCESS! smonkey@glitchcloud.com was able to authenticate to the Microsoft 365 Web Portal.
Checking MFA now...
[**] It appears there is no MFA for this account.
[***] NOTE: Login with a web browser to https://outlook.office365.com using a mobile user agen
t.

----- Microsoft 365 ActiveSync -----
[*] Authenticating to Microsoft 365 Active Sync...
[*] SUCCESS! smonkey@glitchcloud.com successfully authenticated to O365 ActiveSync.
[***] NOTE: The Windows 10 Mail app can connect to ActiveSync.
PS C:\Users\beau\Desktop>

```

```
##### SINGLE FACTOR ACCESS RESULTS #####
Microsoft Graph API | NO
Microsoft Service Management API | NO
O365 w/ Windows UA | NO
O365 w/ Linux UA | YES
O365 w/ MacOS UA | NO
O365 w/ Android UA | YES
O365 w/ iPhone UA | YES
O365 w/ Windows Phone UA | NO
Exchange Web Services | NO
Active Sync | NO
```

Usage

This command will use the provided credentials and attempt to authenticate to the Microsoft Graph API, Azure Service Management API, Microsoft 365 Exchange Web Services, Microsoft 365 Web Portal with both a desktop browser and mobile, and Microsoft 365 Active Sync.

```
1 Invoke-MFASweep -Username targetuser@targetdomain.com -Password
  Winter2020
```

This command runs with the default auth methods and checks for ADFS as well.

```
1 Invoke-MFASweep -Username targetuser@targetdomain.com -Password
  Winter2020 -Recon -IncludeADFS
```

Individual Modules

Each individual module can be run separately if needed as well.

Microsoft Graph API

```
1 Invoke-GraphAPIAuth -Username targetuser@targetdomain.com -Password
  Winter2020
```

Azure Service Management API

```
1 Invoke-AzureManagementAPIAuth -Username targetuser@targetdomain.com -
  Password Winter2020
```

Microsoft 365 Exchange Web Services

```
1 Invoke-EWSAuth -Username targetuser@targetdomain.com -Password
  Winter2020
```

Microsoft 365 Web Portal

```
1 Invoke-0365WebPortalAuth -Username targetuser@targetdomain.com -
  Password Winter2020
```

Microsoft 365 Web Portal w/ Mobile User Agent

```
1 Invoke-0365WebPortalAuthMobile -Username targetuser@targetdomain.com -
  Password Winter2020
```

Microsoft 365 Active Sync

```
1 Invoke-0365ActiveSyncAuth -Username targetuser@targetdomain.com -
  Password Winter2020
```

ADFS

```
1 Invoke-ADFSAuth -Username targetuser@targetdomain.com -Password
  Winter2020
```