

Module 19: Cloud Computing

Lab 1: Perform Reconnaissance on Azure

Lab Scenario

As an ethical hacker, you need to know how to utilize PowerShell command-based scripting tools for conducting reconnaissance and gathering information. This information can then be used to assess the security posture of other systems within the network.

Lab Objectives

- Azure Reconnaissance with AADInternals

Overview of Reconnaissance Tools

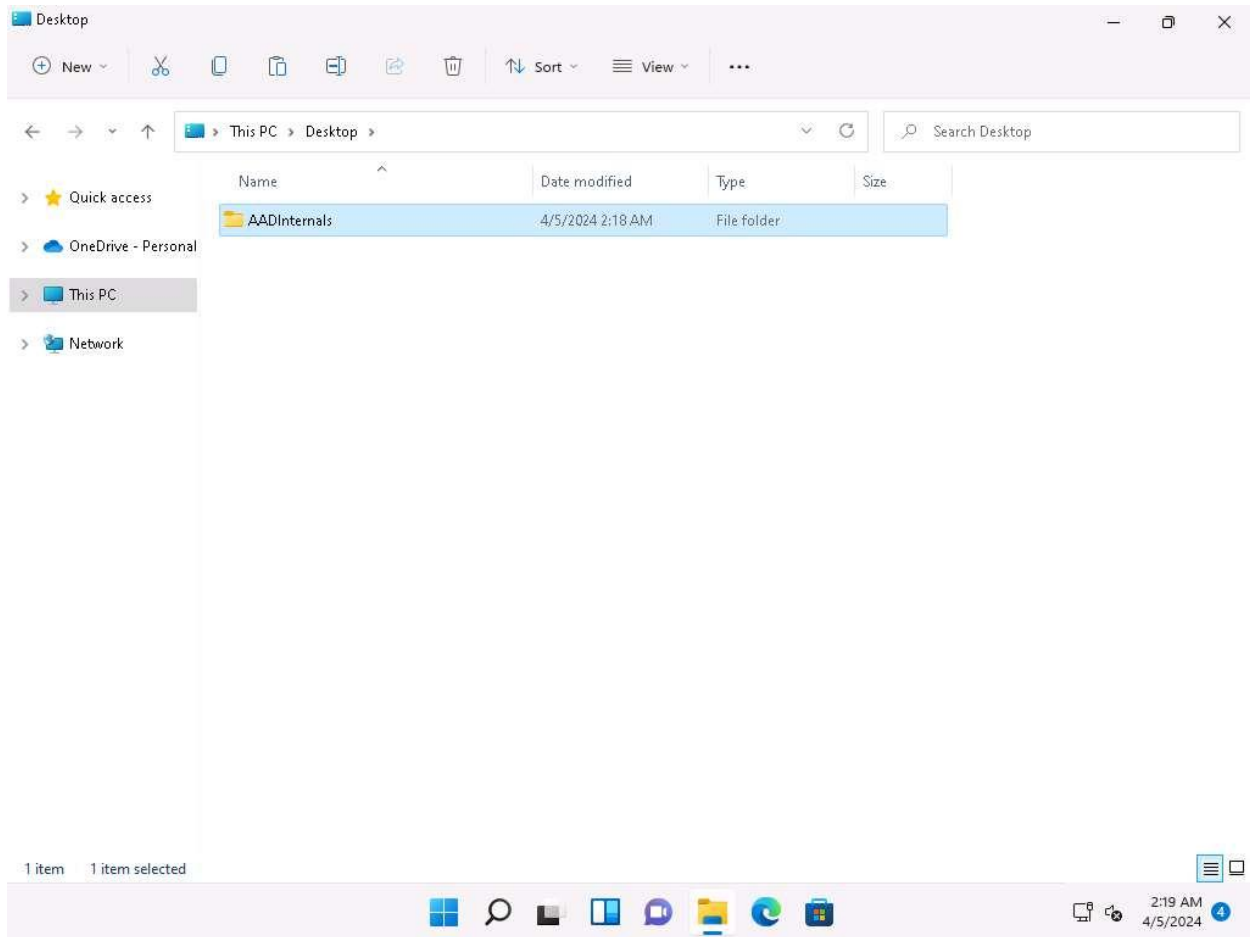
Reconnaissance tools serve as indispensable assets for attackers in cloud hacking, providing them with the essential information and insights needed to orchestrate successful attacks against cloud environments.

Task 1: Azure Reconnaissance with AADInternals

AADInternals is primarily focused on auditing and attacking Azure Active Directory (AAD) environments, it can still be utilized as part of a broader cloud reconnaissance effort. This tool has several features such as user enumeration, credential extraction, token extraction and manipulation, privilege escalation, etc.

In this lab we will perform Azure Active Directory reconnaissance as an outsider.

1. Click [Windows 11](#) to switch to the **Windows 11** machine. Click [Ctrl+Alt+Delete](#) to activate the machine and login with **Admin/Pa\$\$w0rd**.
2. Navigate to **E:\CEH-Tools\CEHv13 Module 19 Cloud Computing\GitHub Tools** and copy **AADInternals** folder and paste it on **Desktop**.



3. In the Windows search type **powershell** and under **PowerShell** click on **Run as Administrator** to open an administrator PowerShell window.

If a **User Account Control** window appears, click **Yes**.

4. In the PowerShell window run **cd C:\Users\Admin\Desktop\AADInternals** command to navigate to **AADInternals** folder.
5. In the PowerShell window run **Install-Module AADInternals** command to install AADInternals module.

In the **Do you want PowerShellGet to install and import the NuGet provider now?** Question type **Y** and press **Enter**. In the **Are you sure you want to install the modules from "PSGallery"?** question type **A** and press **Enter**.

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

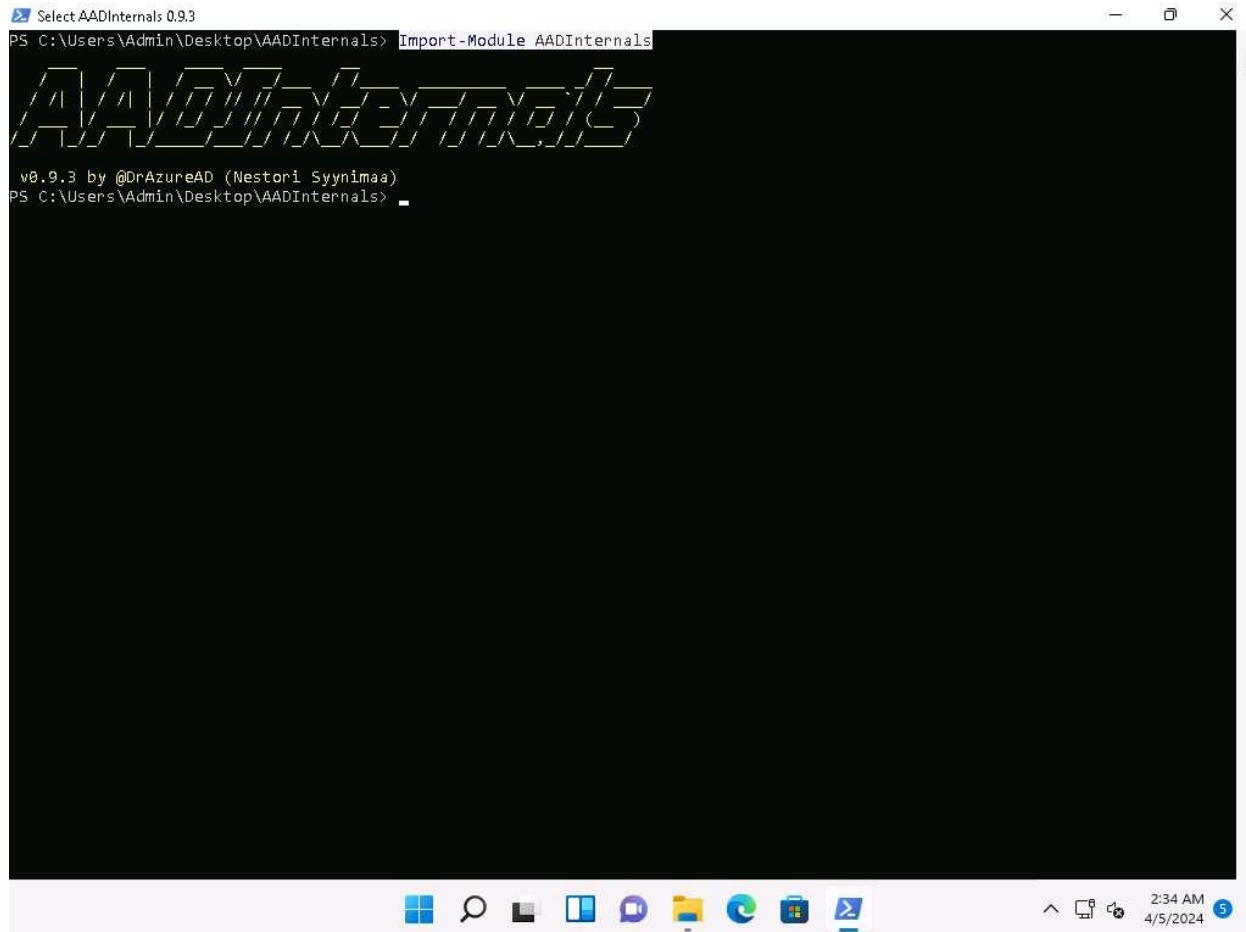
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Windows\system32> cd C:\Users\Admin\Desktop\AADInternals
PS C:\Users\Admin\Desktop\AADInternals> Install-Module AADInternals

NuGet provider is required to continue
PowerShellGet requires NuGet provider version '2.8.5.201' or newer to interact with NuGet-based repositories. The NuGet
provider must be available in 'C:\Program Files\PackageManagement\ProviderAssemblies' or
'C:\Users\Admin\AppData\Local\PackageManagement\ProviderAssemblies'. You can also install the NuGet provider by running
'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'. Do you want PowerShellGet to install and import the
NuGet provider now?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its InstallationPolicy
value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from 'PSGallery'?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): A
PS C:\Users\Admin\Desktop\AADInternals> _
```

6. Now, run **Import-Module AADInternals** command, to import **AADInternals** module.



```
SelectAADInternals 0.9.3
PS C:\Users\Admin\Desktop\AADInternals> Import-Module AADInternals

AADInternals

v0.9.3 by @DrAzureAD (Nestori Syynimaa)
PS C:\Users\Admin\Desktop\AADInternals>
```

7. Now, we will gather the publicly available information of a target Azure AD such as Tenant brand, Tenant name, Tenant ID along with the names of the verified domains.
8. In the PowerShell window run **Invoke-AADIntReconAsOutsider -DomainName company.com | Format-table** command.

In the above command replace the company.com with the target company's domain (here, we are using eccouncil.org).

```
SelectAADInternals 0.9.3
PS C:\Users\Admin\Desktop\AADInternals> Invoke-AADIntReconAsOutsider -DomainName eccouncil.org | Format-table
Tenant brand:      EC-Council
Tenant name:       ECCouncilAbq.onmicrosoft.com
Tenant id:         307907f7-4bb6-4f16-a67d-b9fb26158293
Tenant region:     NA
DesktopSSO enabled: False

Name                DNS    MX    SPF  DMARC  DKIM  MTA-STS  Type    STS
----                -
cisomag.com         True  False True   True   True   False    Managed
cyberq.io           True  False True   False  False  False    Managed
cyberresearch.eccouncil.org True  True  True   False  False  False    Managed
cybersecurity-iclass.eccouncil.org True  False False  False  False  False    Managed
docserver.eccouncil.org True  False True   False  False  False    Managed
eccouncil.org        True  True  True   True   True   False    Managed
ECCouncilAbq.mail.onmicrosoft.com True  True  True   False  False  False    Managed
ECCouncilAbq.onmicrosoft.com True  True  True   False  False  False    Managed
egs.eccouncil.org   True  True  False False  False  False    Managed
examspecialists.com True  True  True   True   True   False    Managed
iibcouncil.org      True  False True   True   True   False    Managed
library.eccouncil.org True  False False  False  False  False    Managed
shieldalliance.com  True  True  True   True   True   False    Managed

PS C:\Users\Admin\Desktop\AADInternals> 
```

9. From the above screenshot we can gather information such as **DNS**, **MX**, **SPF**, **DMARC**, **DKIM** etc.

10. Now, we will perform user enumeration in Azure AD, in the PowerShell window type **Invoke-AADIntUserEnumerationAsOutsider -UserName user@company.com** and press **Enter**.

In the above command replace the user@company.com with the target users email address.

```
AADInternals 0.9.3
PS C:\Users\Admin\Desktop\AADInternals> Invoke-AADIntUserEnumerationAsOutsider -UserName k@eccouncil.org

UserName      Exists
-----
k@eccouncil.org True

PS C:\Users\Admin\Desktop\AADInternals>
```

11. We can see that the result appears, **True** under **Exists** field which implies that the Azure account with the given username exists and the attacker can perform further attacks.
12. We can also perform the user enumeration by placing the usernames in a text file, by running **Get-Content .\users.txt | Invoke-AADIntUserEnumerationAsOutsider -Method Normal**. Where the users.txt file contains the target email addresses.
13. Now, to get login information for a domain type **Get-AADIntLoginInformation -Domain company.com** and press **Enter**.

In the above command replace the company.com with the target company's domain (here, we are using eccouncil.org).

```
SelectAADInternals 0.9.3
PS C:\Users\Admin\Desktop\AADInternals> Get-AADIntLoginInformation -Domain eccouncil.org

Has Password           : True
Federation Protocol    : 
Pref Credential        : 1
Consumer Domain       : 
Cloud Instance audience urn : urn:federation:MicrosoftOnline
Authentication Url     : 
Throttle Status       : 0
Account Type          : Managed
Federation Active Authentication Url : 
Exists                : 1
Federation Metadata Url : 
Desktop Sso Enabled   : 
Tenant Banner Logo    : https://aadcdn.msauthimages.net/dbd5a2dd-vr1b0buqdhxox5jqyhrpb5-9r18ndfouniwh6zqtu/
                        logintenantbranding/0/bannerlogo?ts=636842772025334280
Tenant Locale         : 0
Cloud Instance        : microsoftonline.com
State                 : 4
Domain Type           : 3
Domain Name           : eccouncil.org
Tenant Banner Illustration : https://aadcdn.msauthimages.net/dbd5a2dd-vr1b0buqdhxox5jqyhrpb5-9r18ndfouniwh6zqtu/
                        logintenantbranding/0/illustration?ts=636844291552047322
Federation Brand Name  : EC-Council
Federation Global Version : 
User State            : 1

PS C:\Users\Admin\Desktop\AADInternals>
```

14. Now, to get login information for a user type **Get-AADIntLoginInformation -Domain user@company** and press **Enter**.

In the above command replace the user@company.com with the target users email address.

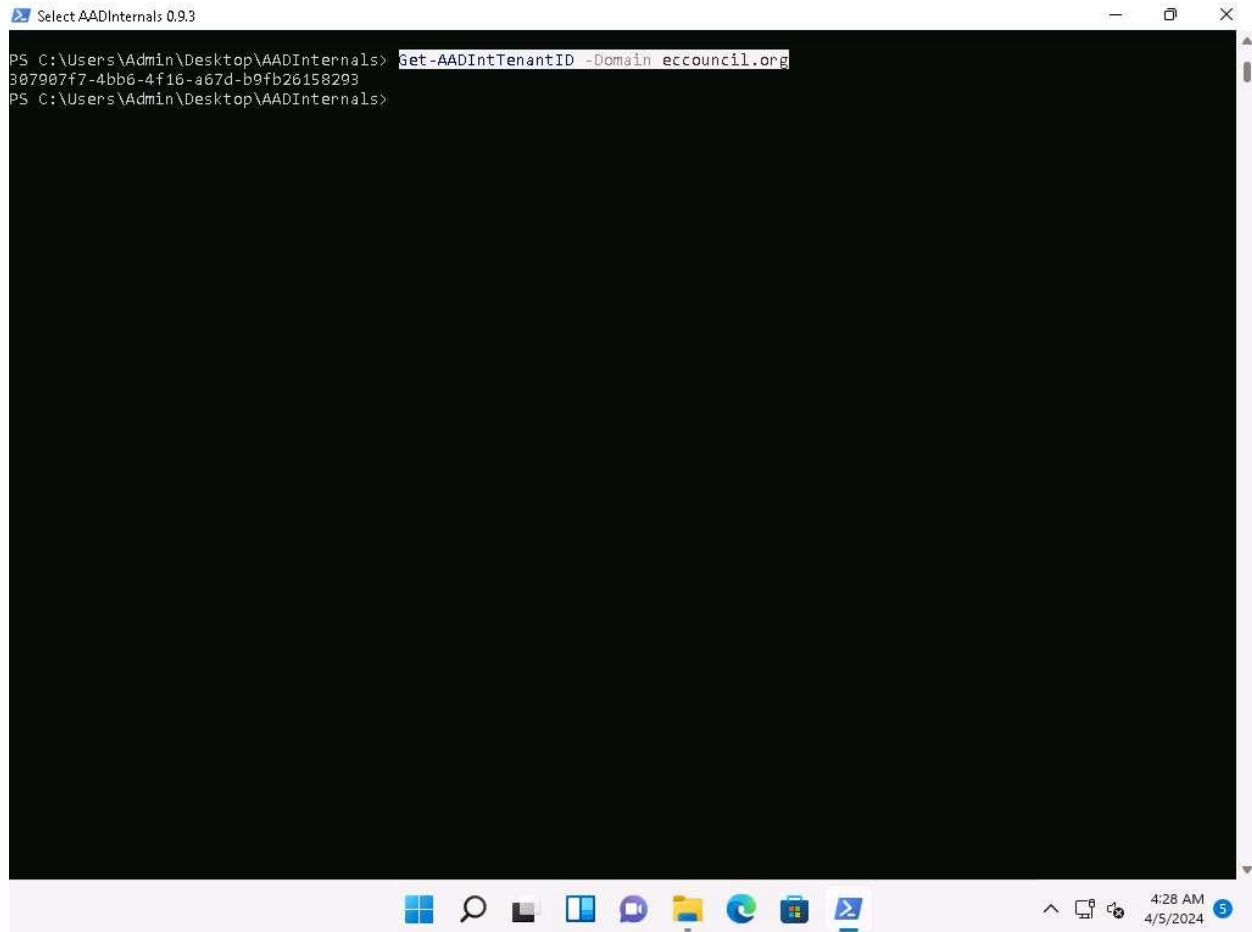
```
AADInternals 0.9.3
PS C:\Users\Admin\Desktop\AADInternals> Get-AADIntLoginInformation -Domain g@eccouncil.org

Has Password           : True
Federation Protocol    : 
Pref Credential        : 1
Consumer Domain        : 
Cloud Instance audience urn : urn:federation:MicrosoftOnline
Authentication Url      : 
Throttle Status        : 1
Account Type           : Unknown
Federation Active Authentication Url : 
Exists                 : 4
Federation Metadata Url : 
Desktop Sso Enabled    : 
Tenant Banner Logo     : 
Tenant Locale          : 
Cloud Instance         : microsoftonline.com
State                  : 4
Domain Type            : 1
Domain Name            : 
Tenant Banner Illustration : 
Federation Brand Name  : 
Federation Global Version : 
User State             : 1

PS C:\Users\Admin\Desktop\AADInternals> _
```

15. To get the tenant ID for the given user, domain, or Access Token, type **Get-AADIntTenantID -Domain company.com**.

In the above command replace the company.com with the target company's domain (here, we are using eccouncil.org).



```
SelectAADInternals 0.9.3
PS C:\Users\Admin\Desktop\AADInternals> Get-AADIntTenantID -Domain eccouncil.org
307907f7-4bb6-4f16-a67d-b9fb26158293
PS C:\Users\Admin\Desktop\AADInternals>
```

16. To get registered domains from the tenant of the given domain **Get-AADIntTenantDomains - Domain company.com**

In the above command replace the company.com with the target company's domain (here, we are using eccouncil.org).

```
SelectAADInternals 0.9.3
PS C:\Users\Admin\Desktop\AADInternals> Get-AADIntTenantDomains -Domain eccouncil.org
cismag.com
cyberq.io
cyberresearch.eccouncil.org
cybersecurity-iclass.eccouncil.org
docserver.eccouncil.org
eccouncil.org
ECCouncilAbq.mail.onmicrosoft.com
ECCouncilAbq.onmicrosoft.com
egs.eccouncil.org
examspecialists.com
iibcouncil.org
library.eccouncil.org
shieldalliance.com
PS C:\Users\Admin\Desktop\AADInternals>
```

17. We can see that all the domains associated with the tenant will be listed.
18. Alternatively you can visit <https://aadinternals.com/osint/> site and type the tenant ID, domain name, or email to get the openly available information for the given tenant.
19. Launch Firefox browser and go to <https://aadinternals.com/osint/> and type the **domain name** in the search box and click on **Get information** button.

Here we are giving the domain name as eccouncil.org.

20. We will get the Domain information and the list of domains connected with the provided domain name.

OSINT

https://aadinternals.com/osint/

Note: CBA status is valid ONLY if email of an **existing user** is given. Using tenant id, domain name, or email of non-existing user may show false negatives.

Note: AAD Connect cloud sync status may return false negatives.

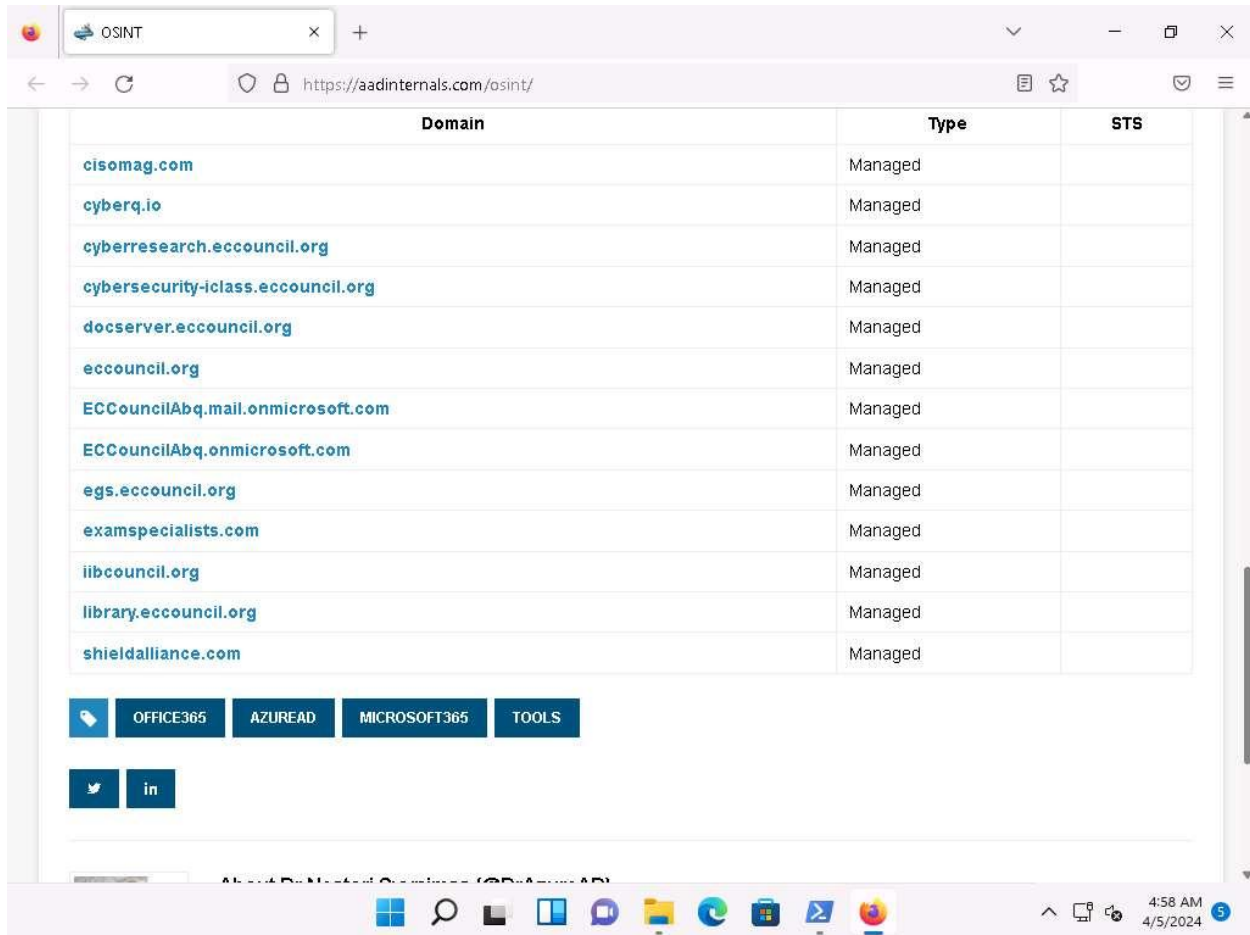
Enter **tenant id, domain name, or email**:

Get information

EC-Council

Property	Value
Default domain	eccouncil.org
Tenant name	ECCouncilAbq.onmicrosoft.com
Tenant brand	EC-Council
Tenant id	307907f7-4bb6-4f16-a67d-b9fb26158293
Tenant region	NA
Seamless single sign-on (SSSO)	disabled
Uses Azure AD Connect cloud sync	N/A
Certificate-based authentication (CBA)	N/A
Verified domains	13

4:58 AM
4/5/2024



21. In similar way you can enter the tenant ID and email in the search field to view the information regarding the tenant and the user.
22. This concludes the demonstration of Azure reconnaissance with AADInternals.
23. Close all open windows and document all acquired information.

Question 19.1.1.1

On windows 11 machine use AADInternals tool located at E:\CEH-Tools\CEHv13 Module 19 Cloud Computing\GitHub Tools\ to perform Reconnaissance on Azure AD. While performing user enumeration in Azure AD what does the Exists field display if the user exists.