Azure Cloud Penetration Testing

Haboob Team

CONTENTS

بسم الله الرحمن الرحيم

WHY CLOUD?

Technology is being fast to change even the idea of keeping tons of servers in that cold room called “Data Center” to perform business applications ,The internet has been going fast in last few years technologies like visualizations helped to improve cloud services , Market numbers of Public cloud computing is getting very big it’s almost getting this year around $355 billion worldwide that huge amount of investments open a expectancy factor why enterprises going to cloud these some of the redone why :

- Budget differential to traditional solutions
- Multi-vendor available Microsoft Azure, Amazon Web Service. Etc...
- Flexible solutions fit all markets
- scalable solutions are already there it can start from small services to huge services

WHY AZURE CLOUD?

If we look at the Global server share by operating system
market in the last two years we will find Microsoft Windows operating system are 72% of the enterprises market that huge amount of infrastructure are designed to work with Microsoft solutions for roadmaps plans Azure will be the suitable choice spatially for System Administrators, Azure has the hybrid choice will take place for those who do not want to throw out there current infrastructure or passably run some secure applications they are not ready to but it on the cloud ,let summery the resin why enterprises will chose Azure :

- flexibility to customers who have Windows infrastructure
- Advance features let the business sucrose
- Infrastructure-as-a-Service(IaaS)and Platform-as-a-Service (PaaS) Capabilities
- High Availability

CLOUD PENETRATION TESTING SCOPE

Doing penetration testing over public cloud is slightly different than on preemies because customers will have different services and there are shared responsibility on security as figure 1 describe how the responsibility shared between service provider and the customer,
Microsoft used to ask for permeations to perform penetration testing on client applications "As of June 15, 2017, Microsoft no longer requires pre-approval to conduct a penetration test against Azure resources."

IaaS- infrastructure as Service	PaaS- Platform as Service	SaaS- Software as Service
User Access Identity	User Access Identity	User Access Identity
Data	Data	Data
Application	Application	Application
Operating System	Operating System	Operating System
Virtualization	Virtualization	Virtualization
Network	Network	Network
Infrastructure	Infrastructure	Infrastructure
Physical	Physical	Physical

Cloud Client / Customer security responsibility
Cloud Provider security responsibility

Figure 1 Shared responsibility security

THE SCOPE OF SECURITY IN PUBLIC CLOUD

Getting detailed in the scope of the engagement is very important for all layers IaaS,PaaS and SaaS however cline side application will take place on IaaS and PasS , here is the 3 layers of scope of public cloud :

1. Account security (permissions, roles, MFA)
2. Cloud Services security like structure storage or Virtual Private Cloud (VPC) misconfiguration
3. Application security include logic or data leak

AZURE STRUCTURE

Azure is cloud computing product from Microsoft it was released in 2010 as "Windows Azure" and was renamed "Microsoft Azure" in 2014 to imply that Azure covers more than just Windows products,
As the figure 2 shows the hierarchy of azure start with
-**Enterprise** account that represents the Azure global account. It's the unique identity that the business owns
-**Tenants** enterprises can have multiple tenants. This is often seen in companies that are geographically separated,
-**Subscriptions** are how you gain access to Azure services (Azure itself, Azure AD, Storage, etc.)
-**Resource Groups** are the containers that house the resources.

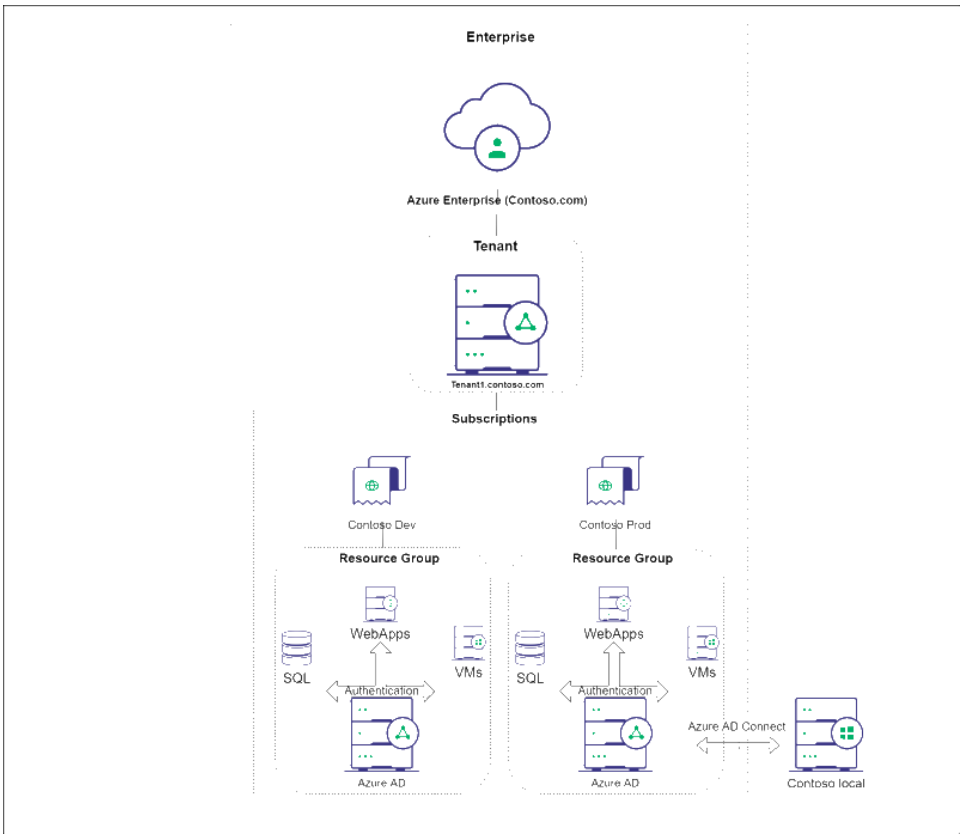
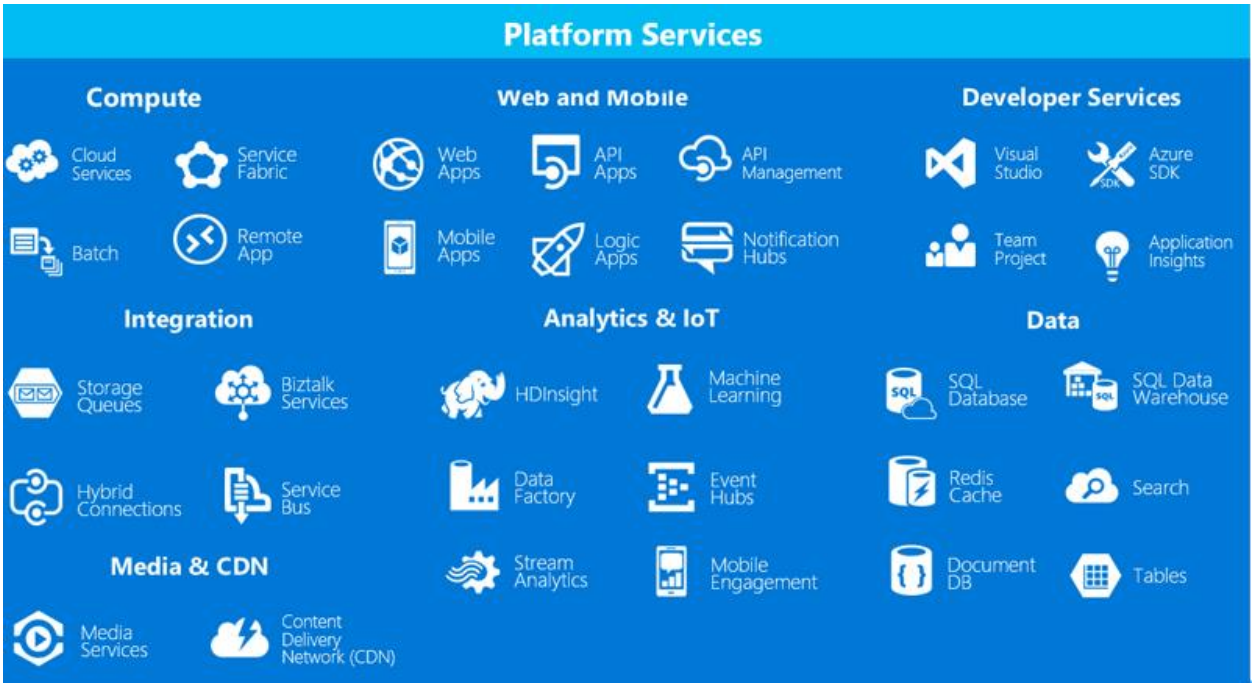


Figure 2 Azure Structure

AZURE SERVICES



Azure have too many services that customer can benefits from we will go through these some interesting services:

- **Azure Storage**

An Azure storage account uses credentials containing an account name and a key. The key is auto-generated when the storage account is created and serves as a password to connect to Azure Storage. The Storage Access keys, by default, has all permissions and is similar to the root password of your storage account.
An Azure storage account contains Blobs, Queues, Tables, and files (shared folder or drive) as storage types and be accessed via an API.

Azure Storage includes these data services:

- Azure Blobs: A massively scalable object store for text and binary data.
- Azure Files: Managed file shares for cloud or on-premises deployments.
- Azure Queues: A messaging store for reliable messaging between application components.
- Azure Tables: A NoSQL store for schemaless storage of structured data.

This four kind has to have permeations from the azure administrator

for pen testers informations from those places will be valuable, Azure Storage Explorer will help you to browse using username and passwords or storage key and name

- Azure AD

Active Directory (AD) is a Microsoft product that consists of several services that run on Windows Server to manage permissions and access to networked resources, to clarify the fuzziness we walk through multiple types:

- **Active Directory Domain Services (on premise)**

Features of Active Directory Domain Services

1. hierarchical directory
2. Extensible schema
3. Store objects like users, computers, groups and security principals
4. Group policy
5. Highly available
6. Support Kerberos ,LDAP and NTLM authentication

- **Azure Active Directory**

Features of Azure Active Directory

1. Cloud based identity
2. Store objects like users, groups , applications and security principals
3. Web based OAuth 2.0 SAML 2.0 and open ID authentication
4. Multi-tenant
5. Flat architecture
6. not extendable
7. No Group policy

- **Azure Active Directory Domain Services**

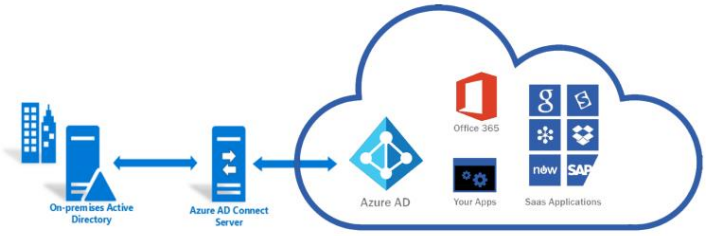
Features of Azure Active Directory Domain Services

1. Cloud posted PasS
2. LDAP, kerberos and NTLM authentication
3. No Domain Admin or Enterprise admin account
4. not extendable schema
5. there are no domain trust
6. LDAP read only

	Active Diroctory Domain Services (on premise)	Azure Active Diroctory	Azure Active Diroctory Domain Services
Extandable schemaN	✓	✗	✗
Group Policies	✓	✗	✓
HA	created by user	✓	✓
Kerberos LDAP,NTLM	✓	✗	✓
oauth,SML Open ID	✗	✓	✗
Dedicated Servers	✓	✗	✗
Cloud Based	aLaS Only	✓	✓
Domain /Enterprize Admin	✓	✗	✗
Domain Forest Trust	✓	✗	✗

Table 2 difference between Active Directory types

Azure AD works fine with web authentication if the hybrid environment would like to sync their credentials should use Azure AD Connect is the Microsoft tool designed to sync hybrid infrastructure identity.



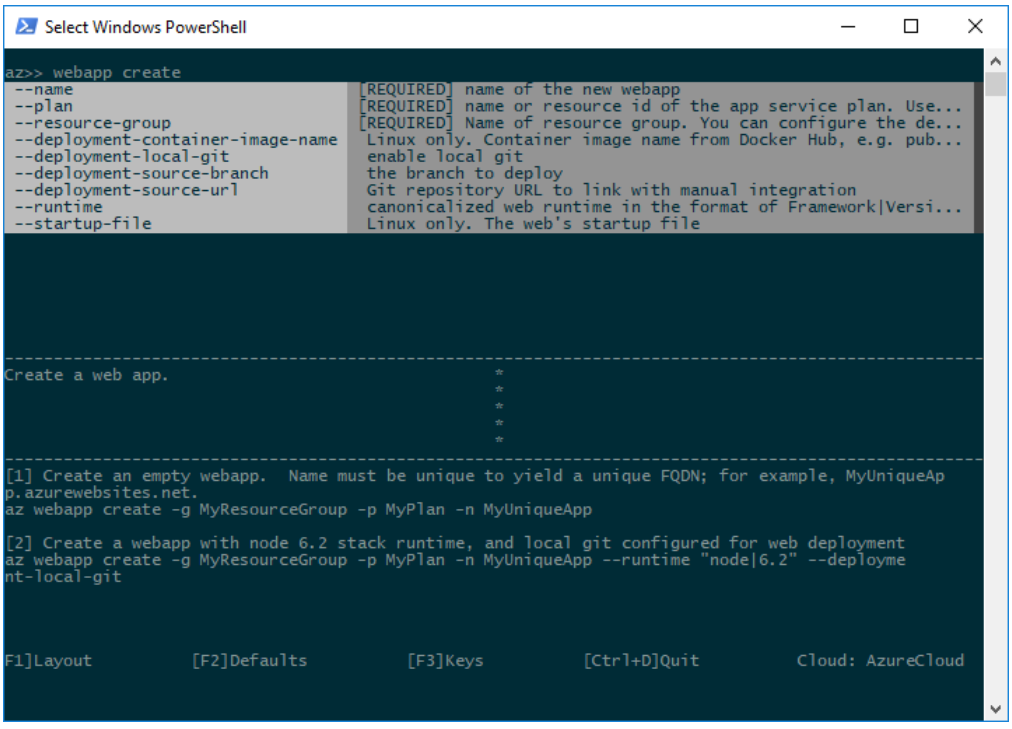
AZURE CLI

Microsoft Azure Command Line Interface is an easy way to manage the account it was designed for administrators an architects how would build scripts and tools to make the process fast as it can be .

Usage
$ az [group] [subgroup] [command] {parameters}

- az - CLI starting point
- az login - log into Azure account
- az account -manage account
- az group -manage resource groups
- az group list -list resource groups

they built an interactive mood that make it easy with auto-completio



AZURE ENUMERATION

Microsoft built the system to help startups and small and medium enterprises they offers domains to for the customers can chose unique name and start with it and then can change it to their domain, Pen tester should manage to find some information about the client in the public subdomains of azure services contains domain name or enterprise name is one of the important point, Take for

example company name “company “should find out that “company” exist on Azure services domains, A list of Azure services domains will be in figure 3 as below

Domain	Associated Service
azurewebsites.net	App Services
scm.azurewebsites.net	App Services - Management
p.azurewebsites.net	App Services
cloudapp.net	App Services
file.core.windows.net	Storage Accounts-Files
blob.core.windows.net	Storage Accounts-Blobs
queue.core.windows.net	Storage Accounts-Queues
table.core.windows.net	Storage Accounts-Tables
redis.cache.windows.net	Databases-Redis
documents.azure.com	Databases-Cosmos DB
database.windows.net	Databases-MSSQL
vault.azure.net	Key Vaults
onmicrosoft.com	Microsoft Hosted Domain
mail.protection.outlook.com	Email
sharepoint.com	SharePoint
azureedge.net	CDN
search.windows.net	Search Appliance
azure-api.net	API Services

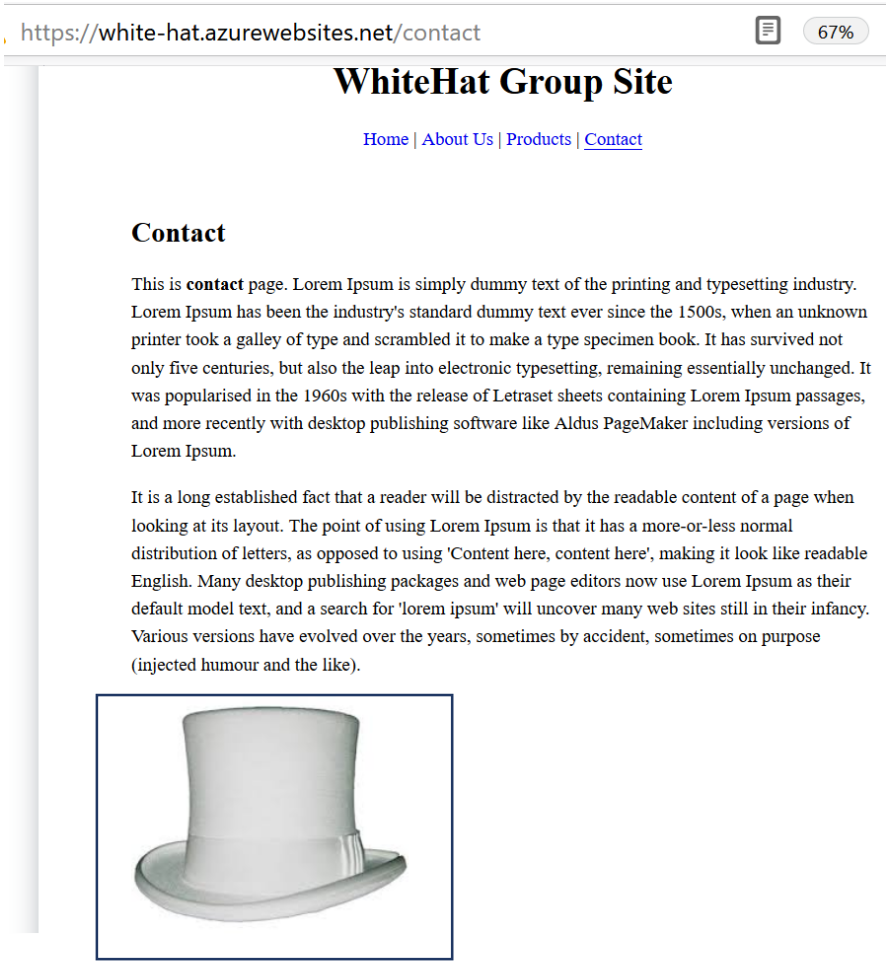
Figure 3 list of Azure services Domains source

There are tools do the job for you for example MicroBurst it will find “company” services if they have already related service to azure

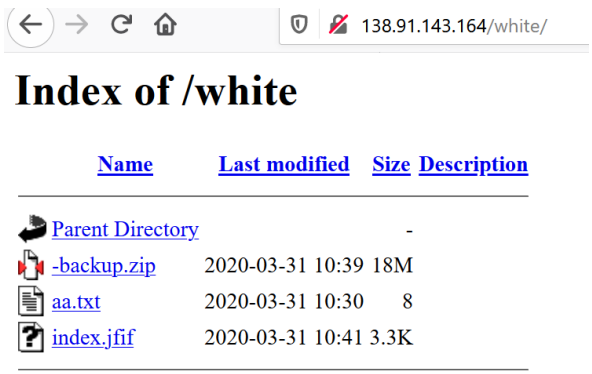
EXAMPLE CASE

Assuming this is a black box pen test we just have the domain of the company "https://white-hat.azurewebsites.net" first looking to the site

1- we found a photo that hosted in server found some useful information there



2- Found a ZIP file named "Backup"

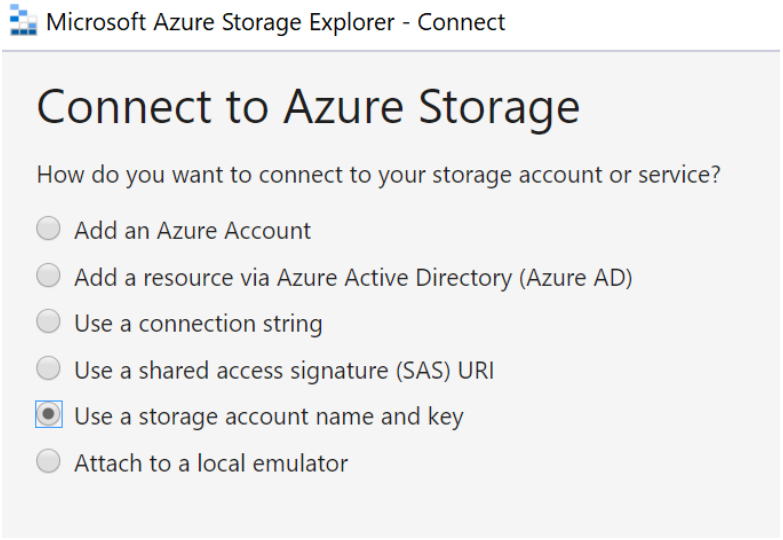


3- Checking the file it looks like it's backup for website let's chick the web.config file we found a key for blob storage

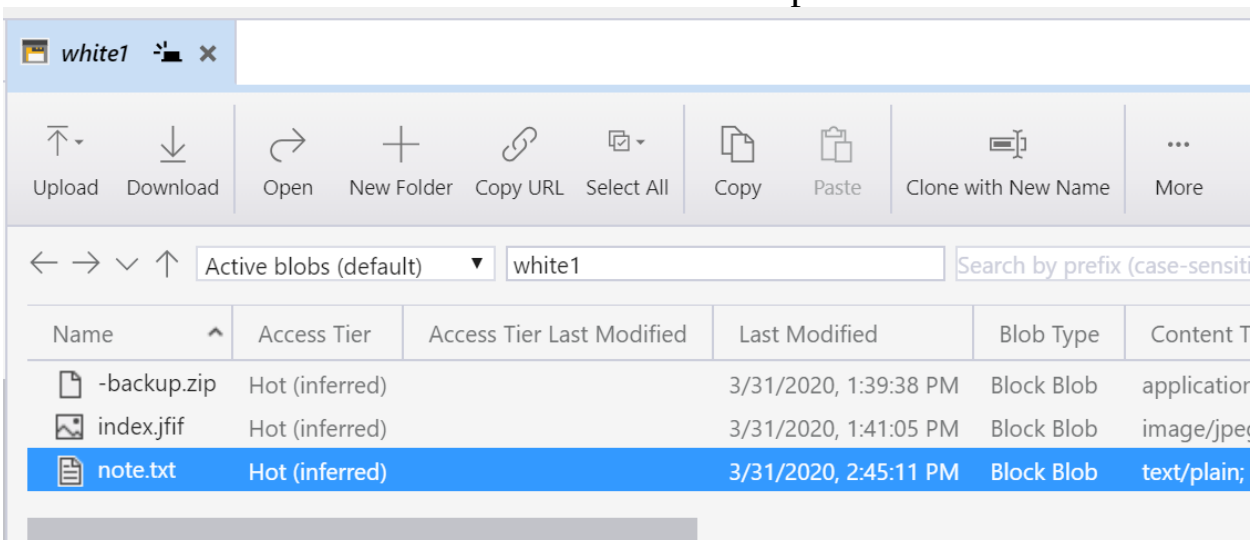
```
ne="ConnectionString"
faultEndpointsProtocol=https;AccountName=witehatt;AccountKey=ExOzahqO2p5EcsOaTc/NzcXCDeDeI95HeeeEAVLzULtK/wPHRpx8NVV7A3XG1A9pCBGh
ame="SqlDev" connectionString="DEVELOPMENT_CONNECTION_STRING" providerName="System.Data.SqlClient"/>
ame="SqlProd" connectionString="PRODUCTION_CONNECTION_STRING" providerName="System.Data.SqlClient"/>
tionStrings>
```

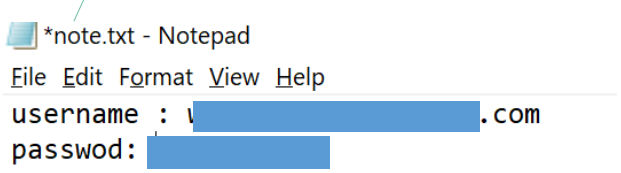
AccountName=witehatt;AccountKey=ExOzahqO2p5EcsOaTc/NzcXCDeDeI95HeeeEAVLzULtK/wPHRpx8NVV7A3XG1A9pCBGhNt2F/PgOujEQoLthXw==;

4- Let's use the Azure Storage Explorer to explore the storage

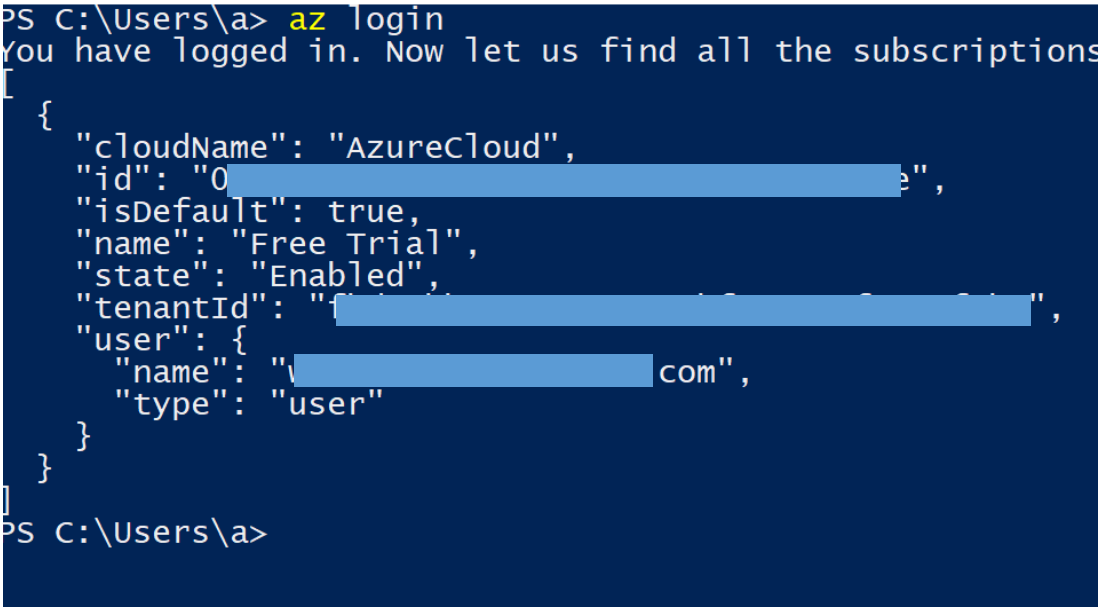


5- Found note.txt has some usernames and passwords





6- Let's connect to Azure CLI using those credentials



7- Done we already in there account we can do whatever

REFERENCES

- https://azure.microsoft.com/en-us/features/storage-explorer/
- https://blog.netspi.com/enumerating-azure-services/
- https://www.statista.com/statistics/915085/global-server-share-by-os/
- https://www.statista.com/topics/1695/cloud-computing/
- https://s3.amazonaws.com/content-production.cloudsecurityalliance/4o2iy0xrw02ldu5zsmt5jnlsgr73?response-content-disposition=inline%3B%20filename%3D%22cloud-penetration-testing-playbook.pdf%22%3B%20filename%2A%3DUTF-8%27%27cloud-penetration-testing-playbook.pdf&response-content-type=application%2Fpdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAJ7D6HHC2YHBAPZ2Q%2F20200318%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20200318T120029Z&X-Amz-Expires=300&X-Amz-SignedHeaders=host&X-Amz-Signature=cf0f0e80d8ed8b8dbb184b7e8ff7bb4e0640efd71a3b738e193c87c56fe2cb26
- https://www.comparex-group.com/web/microsites/microsoft/products/cloud/microsoft-azure/ms-azure.htm