

From Red to Blue

Security Strategies in Azure

whoami

- Anthony Hendricks
 - NSA
 - US Navy/Government Trainer
 - Government and Commercial Penetration Testing/Red Teaming
 - Stage 2 Security / Ultraviolet Cyber
 - Black Hat, BSides Speaker/Trainer

@LoadRemoteLibraryR@infosec.exchange

Azure Basics

- Authentication: Entra ID
- Compute: Virtual machine
- Block Storage: Azure Blobs
- Serverless Applications: Azure Functions
- Container Compute: Container Service
- CDN: Delivery Network
- Data Warehouse: SQL Warehouse

Entra ID (Formerly Azure AD)

What it is:

- Authentication Platform
 - Security Assertion Markup (SAML)
 - Open Authorization (OAuth)
 - Web Service Federation (WS-Fed)
 - OpenID Connect (OIDC)
- User/Permissions Management

What it isn't

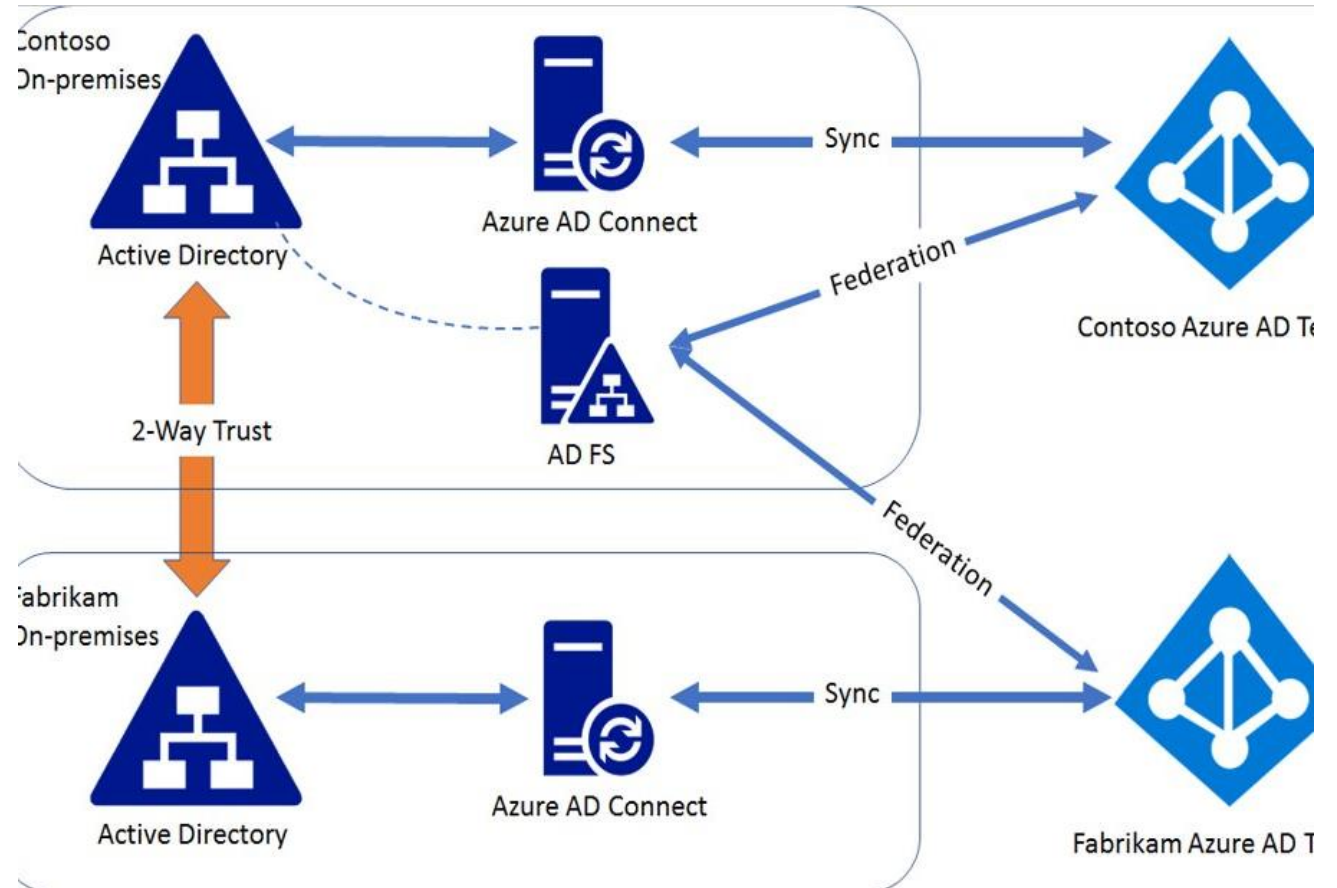
- Active Directory
 - LDAP/Kerberos
 - Tree based organization
 - Group Policy

Entra ID and On-premise Active Directory

- Azure AD-Connect
 - Password Hash Synchronization (PHS)
 - Hash of password hash is stored in Entra ID
 - Password write-back
 - Resilient: Functions if on-prem is down
 - Pass Through Authentication (PTA)
 - All authentication is proxied through on-premise host
 - Fails if on-premise host is down
 - On-premise agent is a target for mimikatz and other attacks

Entra ID and On-premise Active Directory

- Azure AD-Connect
 - Active Directory Federation Services (ADFS)
 - Invite Entra ID to be a tenant of on-premise Active Directory
 - Very few cases where this is necessary



Is a Domain Managed by Entra ID?

<https://login.microsoftonline.com/getuserrealm.srf?login=<user@domain.com>&xml=1>

- Unmanaged

```
▼<RealmInfo Success="true">  
  <State>4</State>  
  <UserState>1</UserState>  
  <Login>username@adomain.com</Login>  
  <NameSpaceType>Unknown</NameSpaceType>  
</RealmInfo>
```

- Managed

```
▼<RealmInfo Success="true">  
  <State>4</State>  
  <UserState>1</UserState>  
  <Login>someuser@uvcyber.com</Login>  
  <NameSpaceType>Managed</NameSpaceType>  
  <DomainName>uvcyber.com</DomainName>  
  <IsFederatedNS>false</IsFederatedNS>  
  <FederationBrandName>UVCyber</FederationBrandName>  
  <CloudInstanceName>microsoftonline.com</CloudInstanceName>  
  <CloudInstanceIssuerUri>urn:federation:MicrosoftOnline</CloudInstanceIssuerUri>  
</RealmInfo>
```

Check for Valid Account Name

- <https://login.microsoftonline.com/common/GetCredentialType>
 - POST Request {"Username":"<someUserName>"}
 - Valid: IfExistsResult:0
 - Invalid: IfExistsResult:1
- See also o365creeper (<https://github.com/LMGsec/o365creeper>)

Service Principals

- Entra ID equivalent of Service Accounts
- Tied to Application Instance
 - Remove the Application Instance, remove the credentials
- Credential Models
 - Username/Password
 - Certificate

Managed Service Identity (MSI)



Managed service identity

lizardblue



Managed service identity

Your application can communicate with other Azure services as itself using a managed Azure Active Directory identity. [Learn more](#)

Register with Azure Active Directory

Off

On

Save

Discard

MSI

Managed Service Identity URL is used to generate a token which can be used when authorizing to other Azure Services. When activating Managed Service Identity on your Function App, two environment settings are added to the configuration of your Function app service.

Use “SET” command to find the storage creds

MSI_ENDPOINT : the local URI for which your app can request tokens

MSI_SECRET: the secret used to request a token from the MSI_ENDPOINT

Often used with Key Vault

```
( _____ ) ( ____ _ )  
  
Manage your web app environment by running common commands  
( 'mkdir', 'cd' to change directories, etc.) This is a sandbox  
environment, so any commands that require elevated privileges will  
not work.
```

```
D:\home\site\wwwroot>set | findstr MSI  
MSI_ENDPOINT=http://127.0.0.1:41077/MSI/token/  
MSI_SECRET=589B050A418E4FC2B4BB571AEA388954
```

```
D:\home\site\wwwroot>
```

Azure Key Vault

Secrets, Keys, Certificate Management

Create a resource group, which is a logical container into which Azure resources are deployed and managed:

- `az group create --name "ContosoResourceGroup" --location eastus`

Create a Key Vault, which is a logical group of secrets:

- `az keyvault create --name "Contoso-Vault2" --resource-group "ContosoResourceGroup" --location eastus`

Add & View a Secret to the Key Vault:


- `az keyvault secret set --vault-name "Contoso-Vault2" --name "ExamplePassword" --value "Pa$$w0rd"`
- `az keyvault secret show --name "ExamplePassword" --vault-name "Contoso-Vault2"`

Three ways to authenticate to Key Vault:

- Managed Identities (aka MSI)
- Service Principal and Certificate
- Service Principal and Secret (aka password)


Consent Grant

- Users and Admins can grant permissions to OAuth Applications
 - Permissions can be active even when the user is not actively using the app

 Microsoft

testadmin@fourthcoffeetest.onmicrosoft.com

Permissions requested

 Best Practices Demo
microsoftidentity.dev

This application is not published by Microsoft or your organization.

This app would like to:

✓ Read all groups

✓ Maintain access to data you have given it access to

✓ View your basic profile

☐ Consent on behalf of your organization

Accepting these permissions means that you allow this app to use your data as specified in their [terms of service](#) and [privacy statement](#). You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

Cancel

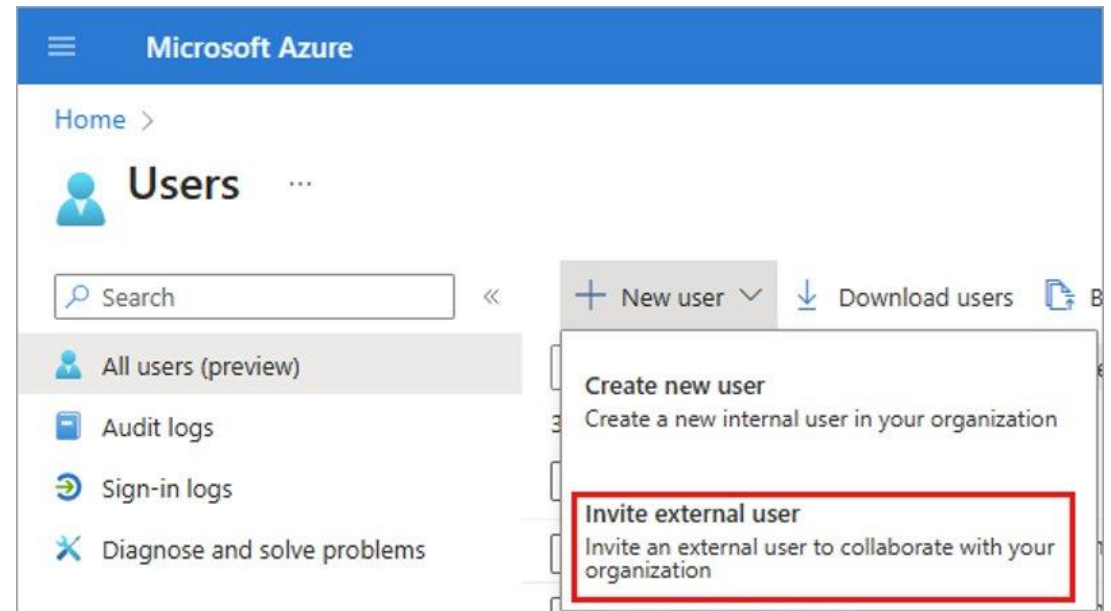
Accept

Consent Grant

- A Phished user may unwittingly provide access to
 - Users and Groups
 - User data such as mail and calendars
 - Service Principals
- Defense
 - Restrict to Publisher Verified Apps (Microsoft publisher validation)
 - Consent workflow for additional scrutiny
 - Audit Applications and permissions

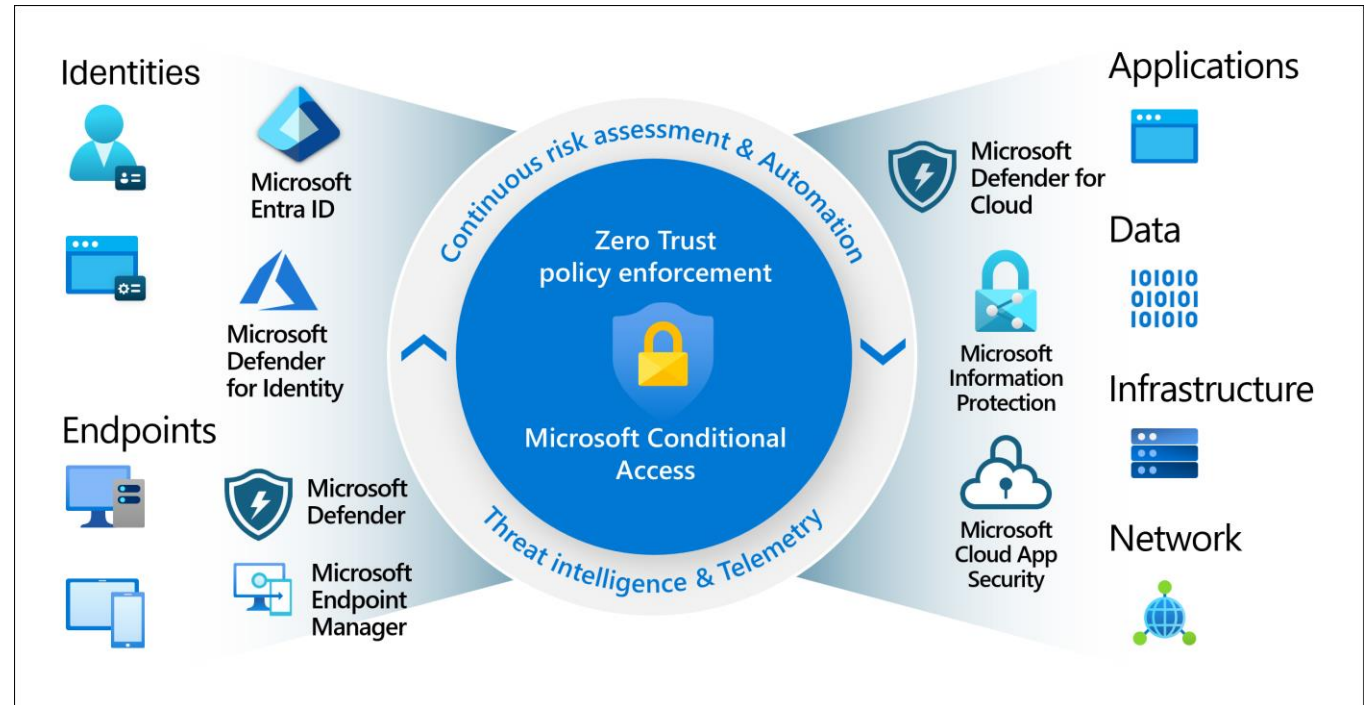
Guests & Guest Sync

- External Users can be invited as Guests and assigned permissions
- An external group can be given access and automatically approved with Cross-tenant Synchronization



Conditional Access

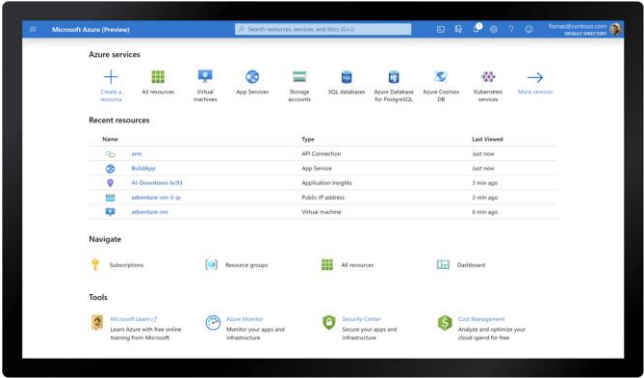
- Criteria for Authentication
 - Source IP/Geo
 - Device type
 - Destination
 - Risk



MFA & Passwordless

- Microsoft Authenticator App
 - Number matching
- SMS/Phone call
- TOTP Token
- Windows Hello with PIN/Biometrics
- FIDO2
- Certificate Based

Azure AD Management APIs



Azure Web Portal



Azure Portal API



Internal Azure AD Graph API

Status	Method	Domain	Path	Type	Transferred	Size	0 ms
200	GET	afd.hosting.portal.a...	zwB...LudD.js	js	6.03 KB	24.14 KB	44 ms
200	POST	portal.azure.com	Delegat...ken?feature.refreshTokenbinding=...	xhr	2.93 KB	6.21 KB	317 ms
200	POST	portal.azure.com	Delegat...ken?feature.refreshTokenbinding=...&featur...	xhr	3.48 KB	6.36 KB	152 ms
200	GET	graph.windows.net	roleDefinition?api-version=1.61-internal&\$top=500	xhr	68.92 KB	68.89 KB	143 ms
200	OPTIONS	main.iam.ad.ext.az...	CurrentContext	xhr	39 B	0 B	95 ms
200	GET	main.iam.ad.ext.az...	CurrentContext	xhr	992 B	99 B	57 ms
200	OPTIONS	main.iam.ad.ext.az...	RoleAssignments?scope=undefined	xhr	752 B	0 B	62 ms

Graphrunner

- Explores Azure and M365 using Graph API
 - Mail/Contacts
 - Teams Content
 - SharePoint
- <https://www.blackhillsinfosec.com/introducing-graphrunner/>

AADInternals

- Hacking Toolkit for Entra ID
 - Graph API
 - Authentication
 - Unauthenticated Recon
- AADInternals.com

Road Tools

- Roadrecon: Data collection tool via Graph API
 - Entra ID
 - Applications
 - Service Principals
- RoadTools GUI: Explore collected data
- <https://github.com/dirkjanm/ROADtools>



Stormspotter

- Developed by Azure Red Team
- Explores and graphs Azure resources
 - Subscriptions
 - Resource Groups

- <https://github.com/Azure/Stormspotter>

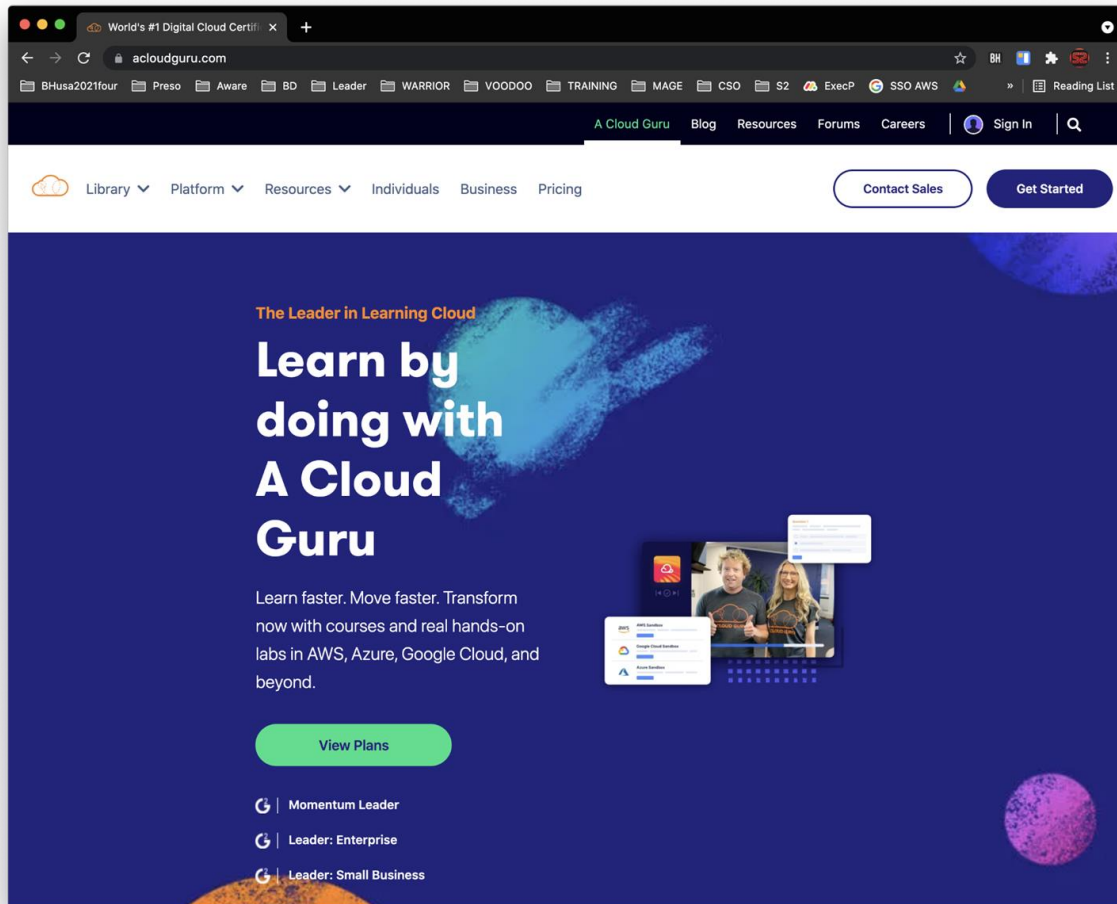


STORMSPOTTER

Guides

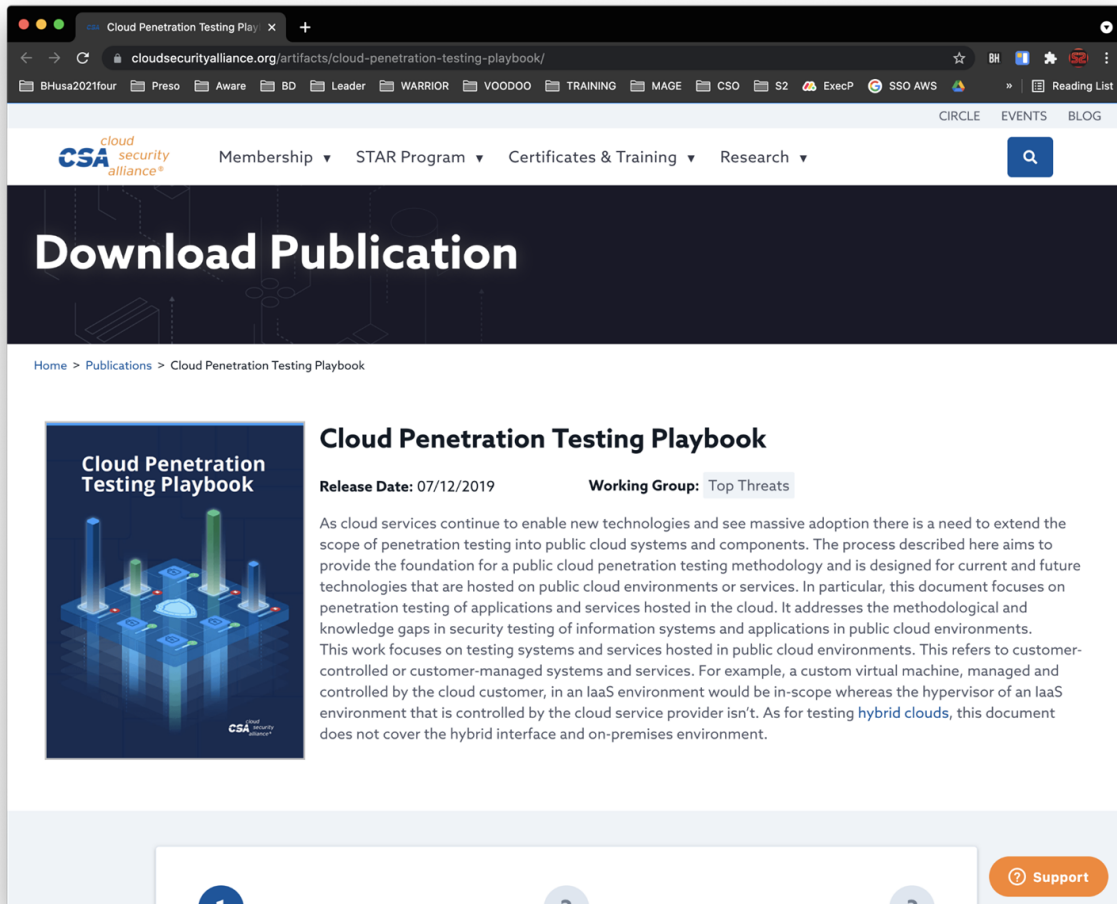
- <https://cloud.hacktricks.xyz/pentesting-cloud/>
- <https://pentestbook.six2dez.com/enumeration/cloud/>
- <https://github.com/dafthack/CloudPentestCheatsheets>
- PayloadsAllTheThings:
 - <https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Cloud%20-%20Azure%20Pentest.md>
- <https://github.com/vengatesh-nagarajan/Cloud-pentest>
- <https://github.com/CyberSecurityUP/Awesome-Cloud-PenTest>
- <https://github.com/kh4sh3i/cloud-penetration-testing>

aCloudGuru.com / Pluralsite



Great Information on
AWS, Azure, GCP, & K8s

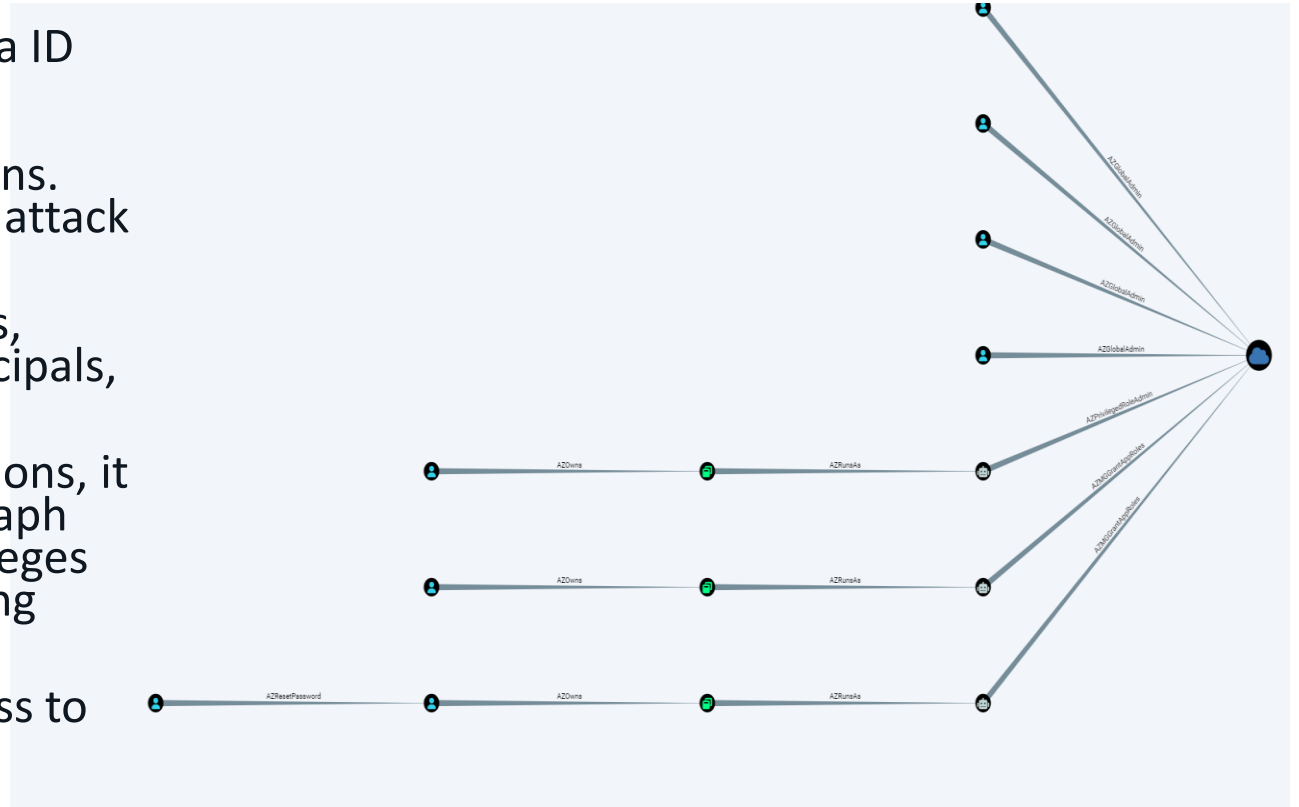
CSA: Cloud Penetration Testing Playbook



The target audience of this document are penetration testers and cloud / cloud-based systems security practitioners. However, the first few pages will provide CIOs, CISOs and Senior Management an understanding of what cloud penetration testing is, its scope, its context, its objectives and how it fits within a cybersecurity strategy. Developers and Architects will also find this document useful while designing secure (public cloud based) systems.

BadZure: Vulnerable Entra ID

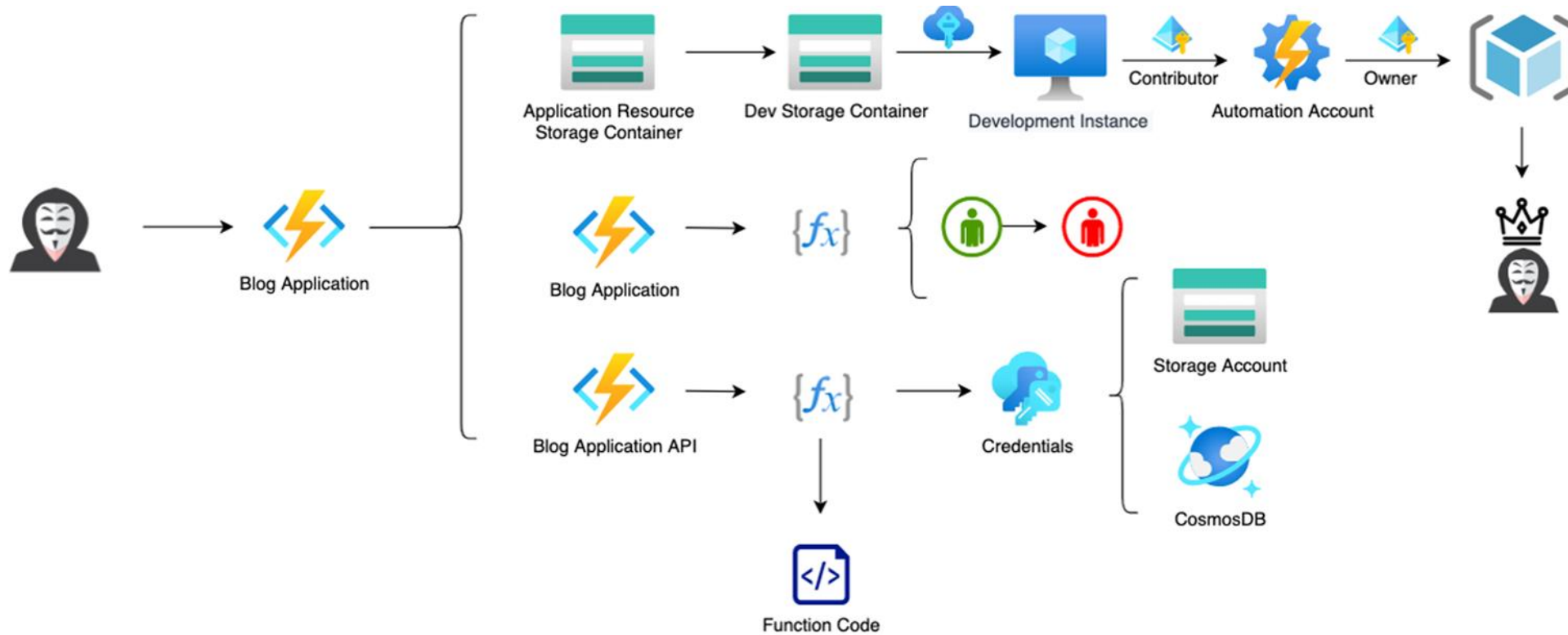
- BadZure is a PowerShell script that uses the Microsoft Graph SDK to set up Microsoft Entra ID (formerly Azure Active Directory) tenants, populating them with various entities and introducing common security misconfigurations. This creates vulnerable tenants with multiple attack paths.
- It automates the creation of entities like users, groups, application registrations, service principals, and administrative units.
- To simulate real-world security misconfigurations, it randomly assigns Microsoft Entra ID roles, Graph permissions, and application ownership privileges to randomly picked security principals, creating unique attack paths.
- BadZure provides two methods of initial access to the vulnerable tenants it creates, simulating account takeover scenarios.
- The tool is designed for security practitioners interested in exploring and understanding Microsoft Entra ID security.



AzureGoat

TL;DR:

- Focused on Azure



Questions?

- Slides will be posted later
 - https://github.com/rDmKW5nQ/2023_Bsides_RedRocks

