David Okeyode

How vulnerable is your Azure environment?

Join virtual on July 28

azureday.community

David Okeyode

- Independent Cloud Security Consultant
- Over a decade of experience in Cybersecurity (consultancy, design, implementation)
- Over 6 years of experience as a trainer
- BLOG: https://azurehangout.com

asegunlolu

@asegunlolu

Microsoft Certified Azure AI Engineer Associate

Microsoft Certified Azure Developer Associate

Microsoft Certified Azure Administrator Associate

Microsoft Certified Azure Security Engineer Associate

Microsoft Certified Azure Solutions Architect Expert

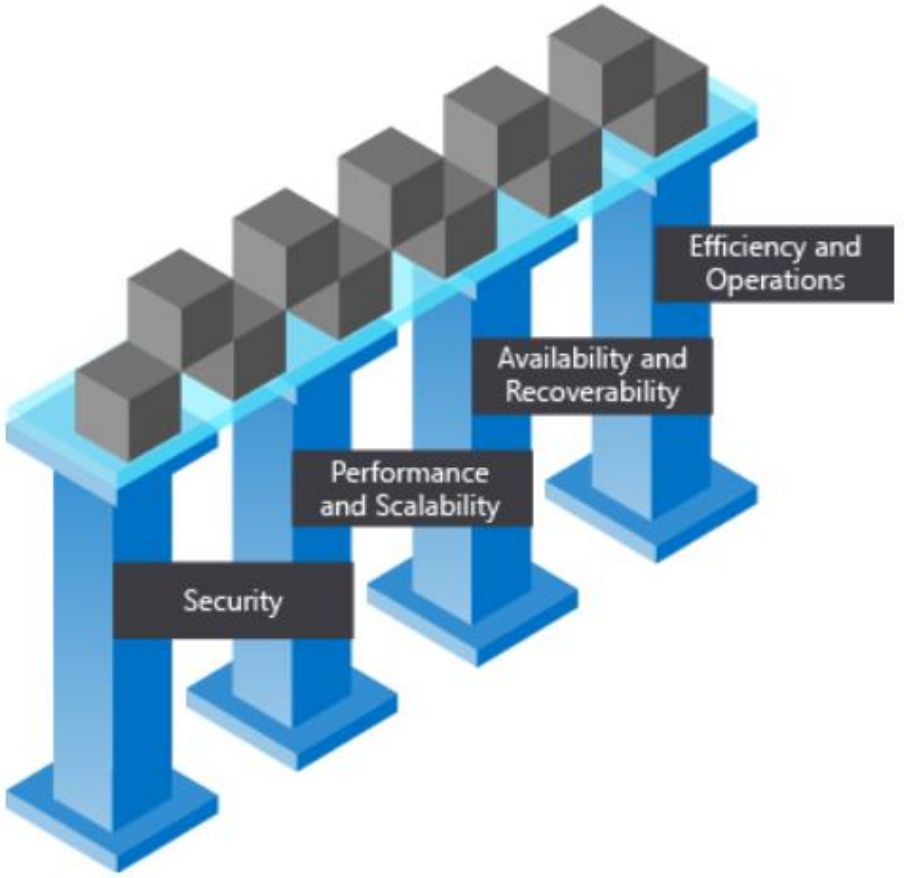
Microsoft Certified Azure DevOps Engineer Expert

AWS certified Solutions Architect Professional

AWS certified Security Specialty

Pillars of a great Azure Architecture

- Security
- Performance and Scalability
- Availability and Recoverability
- Efficiency and Operations



AZURE HANGOUT

Why a different approach?

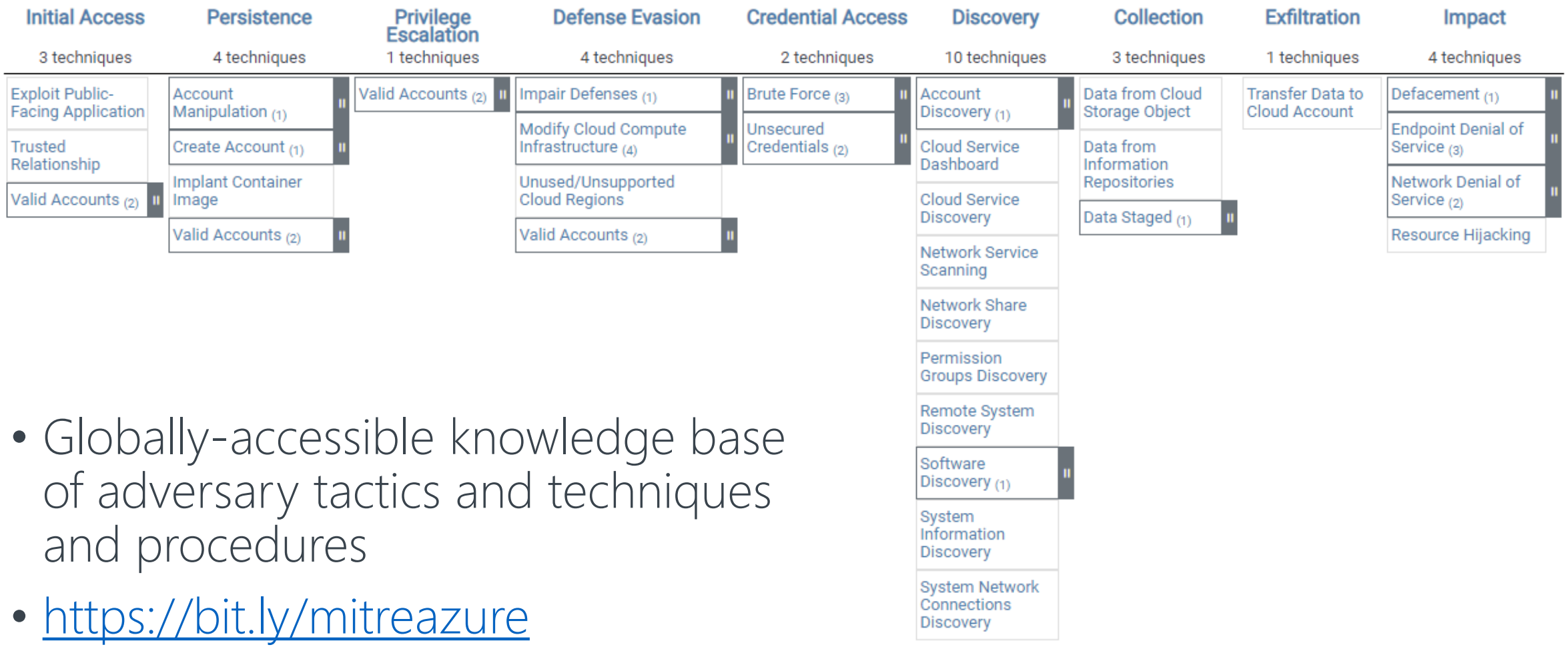
- A lot of presentations, talks and videos already focus on best practices and the use of tools
- Understanding attacker behaviour is an important part of cybersecurity education
- Learn what not to do from the failures of others

Iku to npa ojugba eni, owe nla lo npa fun ni

When death strikes your mate, it sends you a strong message –

– Yoruba Proverb

MITRE ATT&CK® Matrix for the Azure Platform



- Globally-accessible knowledge base of adversary tactics and techniques and procedures
- https://bit.ly/mitreazure

AZURE HANGOUT

Azure Platform Attack Matrix

- Cloud provider IP range network scan
- Cloud provider IP range vulnerability scan
- Cloud Service Discovery
- DNS Brute Force

- Remote code execution
- Password Brute Force Attack

- Exposed cloud account credentials
- Insecure cloud account credentials
- Application vulnerability
- Compromised container images
- Stolen cloud account credentials
- Dependency/Plugin vulnerability

- Source control service scans
- DevOps tools scans
- Credentials in configuration settings
- Credentials in configuration files
- Azure Blob/File Scan
- Harvesting connection strings
- Harvesting API keys

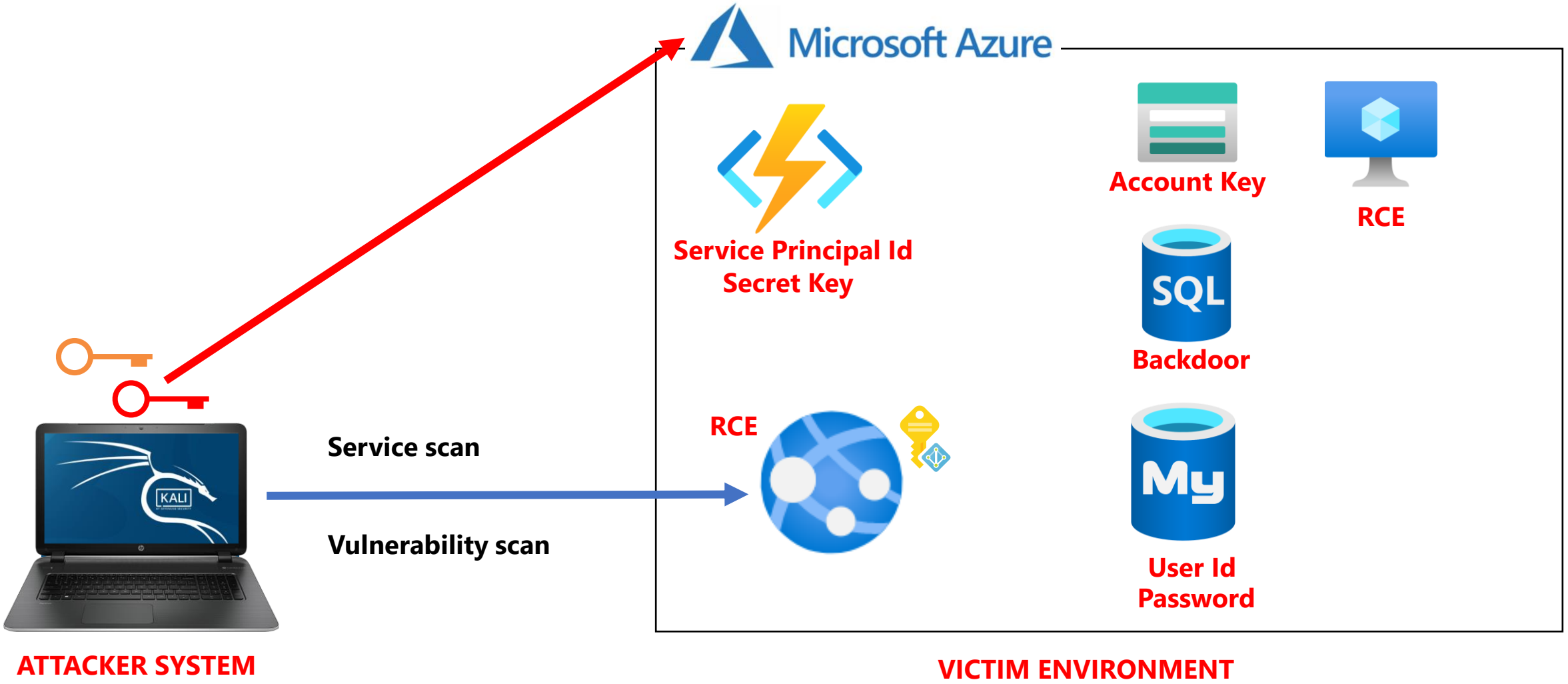
- Privileged EC2 instances
- Cloud Shell Privilege Escalation

- Account manipulation
- Create account
- Implant container image
- Network Security Group Backdoor
- Backdoor Azure function

- Azure Storage Dump
- Azure Disk Snapshot and Download
- Data destruction
- Resource hijacking
- Crypto-mining
- Denial of service

AZURE HANGOUT

Attack Scenario - DEMO



Rules of Engagement and Consequences

https://bit.ly/azurepentest

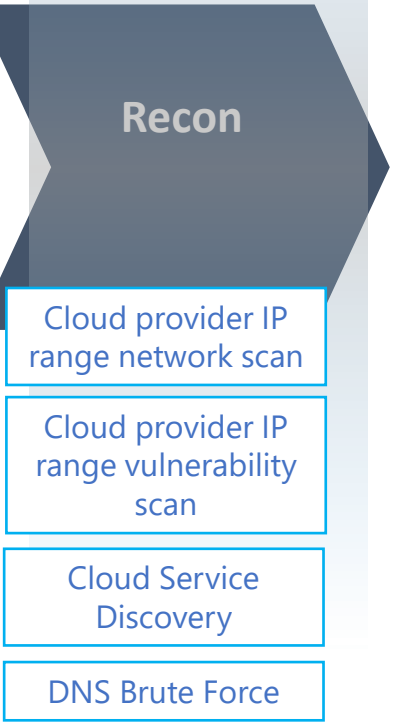
Suspension or termination of our Azure account

Legal action brought against us by Microsoft!

Financial liability for damage to the Microsoft Cloud or customer data

AZURE HANGOUT

Reconnaissance



- Identify potential targets
- Determine target surface area
- Identify target's vulnerabilities

AZURE HANGOUT

Recon – Cloud Provider IP Range Scan

- Azure publishes a list of Azure public IPs

```
# Download a list of Azure public IPs (Public Regions)
wget https://download.microsoft.com/../ServiceTags_Public_20200720.json
```

- Hackers typically parse this list to identify potential targets

```
# Obtain a list of public IP ranges used by services in UKSOUTH
jq -r '.values[] | select(.properties.region=="uksouth") |
select(.properties.platform=="Azure")' < ServiceTags_Public_20200720.json


# Obtain a list of public IP ranges used by the Azure App Service in the UKSOUTH region
jq -r '.values[] | select(.properties.region=="uksouth") |
select(.properties.platform=="Azure") |
select(.properties.systemService=="AzureAppService") |
.properties.addressPrefixes' < ServiceTags_Public_20200720.json
```

AZURE HANGOUT

Recon – Cloud Service Discovery

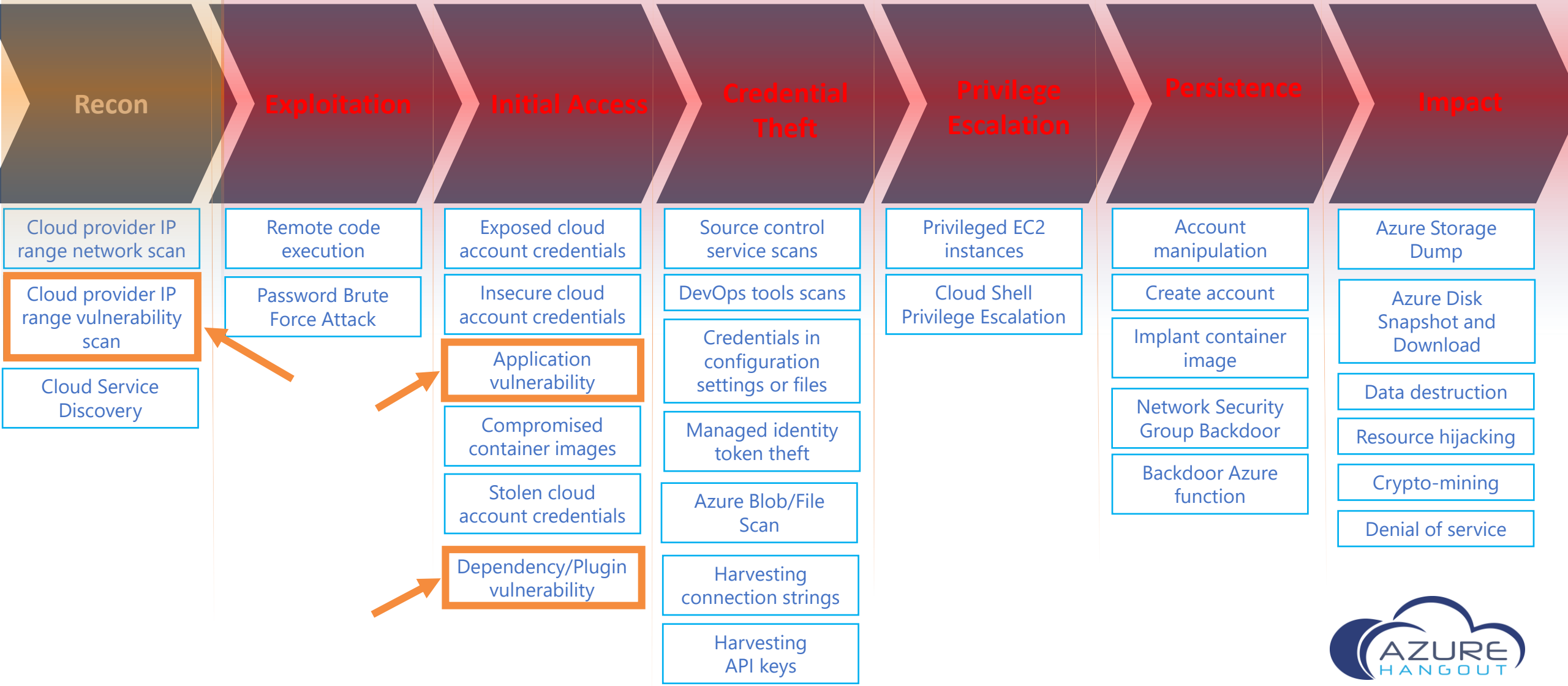
- Microsoft makes several domains/subdomains for Azure platform services

DNS Suffix	Associated Service
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
azureedge.net	CDN
search.windows.net	Search Appliance
servicebus.windows.net	Service Bus and Event Hub
.redis.cache.windows.net	Azure Cache for Redis

Recon – Cloud Service Discovery

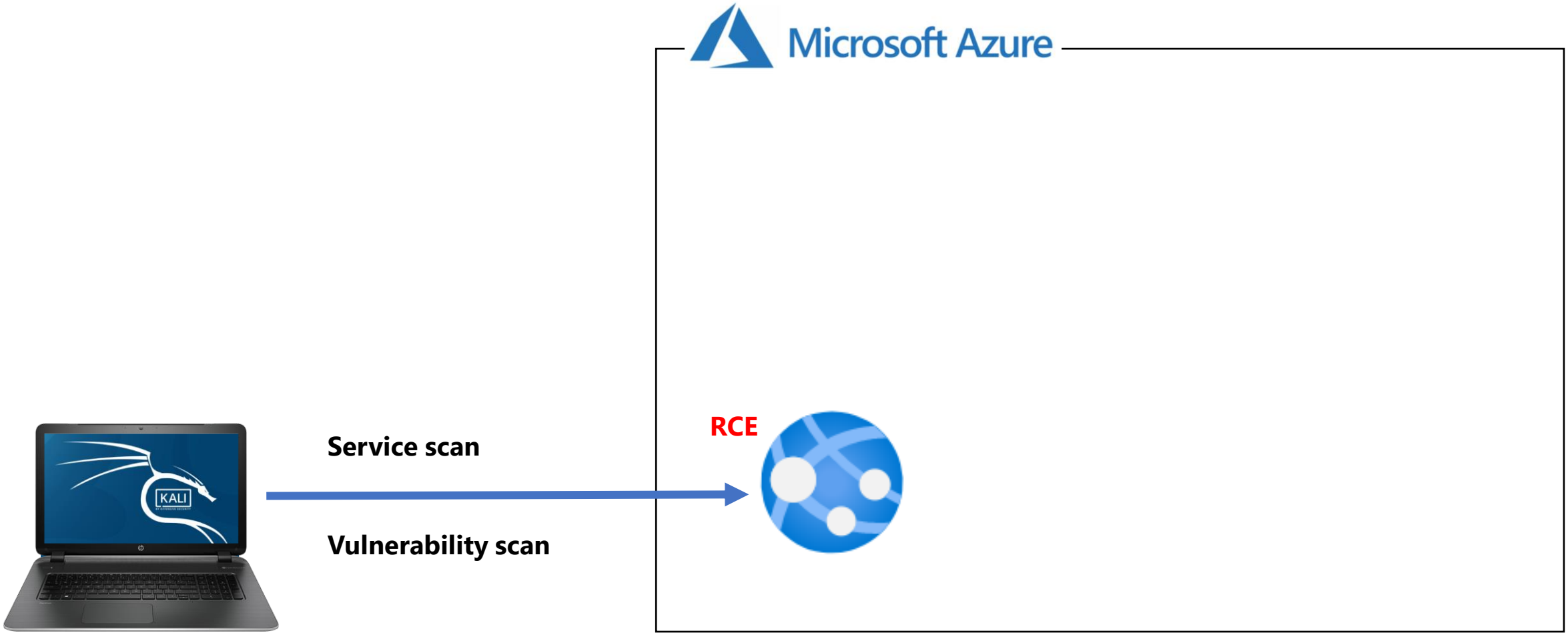
- DNS enumeration
- Querying search engines
  - site:.blob.core.windows.net
  - site:.azure-api.net
- Performing DNS brute force discovery
  - AMASS
  - SubBrute
  - Knock
  - DNSRecon
  - Sublist3r
  - AltDNS
- This is just information gathering and not a vulnerability (security loophole)

Azure Platform Attack Matrix



AZURE HANGOUT

Attack Scenario - DEMO



Credential Theft

Credential Theft

- Source control service scans
- DevOps tools scans
- Credentials in configuration settings or files
- Managed identity token theft
- Azure Blob/File Scan
- Harvesting connection strings
- Harvesting API keys

- Techniques for stealing credentials like account names passwords and tokens
- Techniques that are used on-premises applies here. But there are some techniques that are also unique to an environment like Azure
- Credentials in configuration settings E.g. App service settings
- Managed identity token theft

AZURE HANGOUT

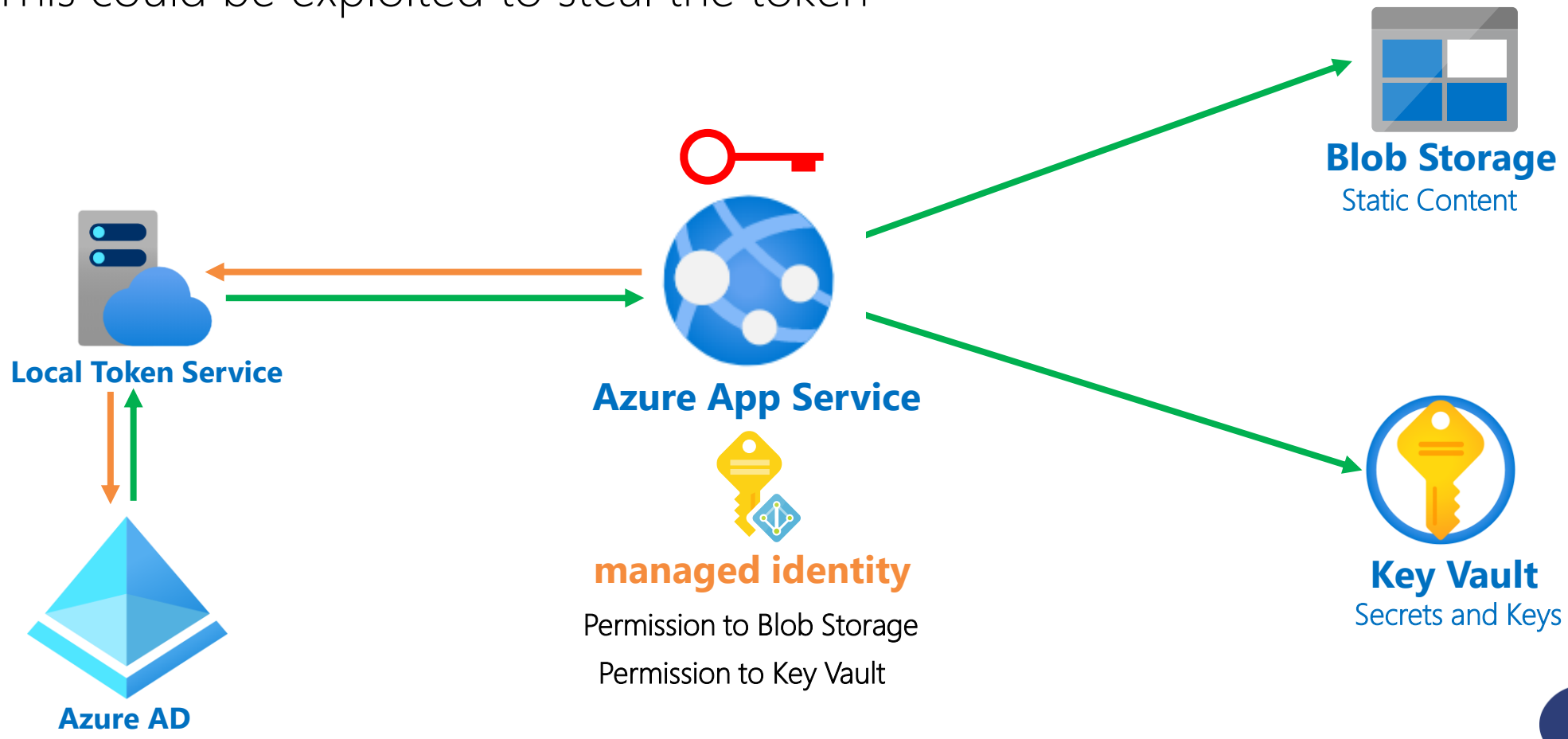
Azure App Service Settings

- Used to pass variables as environment variables to application code
- Any value passed can be dumped locally using “printenv” (for Linux service plans)
- Presence of IDENTITY_HEADER and IDENTITY_ENDPOINT environment variables indicates that a managed identity is associated

AZURE HANGOUT

Managed Identity

- Applications hosted on services like Azure App Service and Azure Functions needs to access other Azure services
- The more secure way to implement this is to use a managed identity
- This could be exploited to steal the token

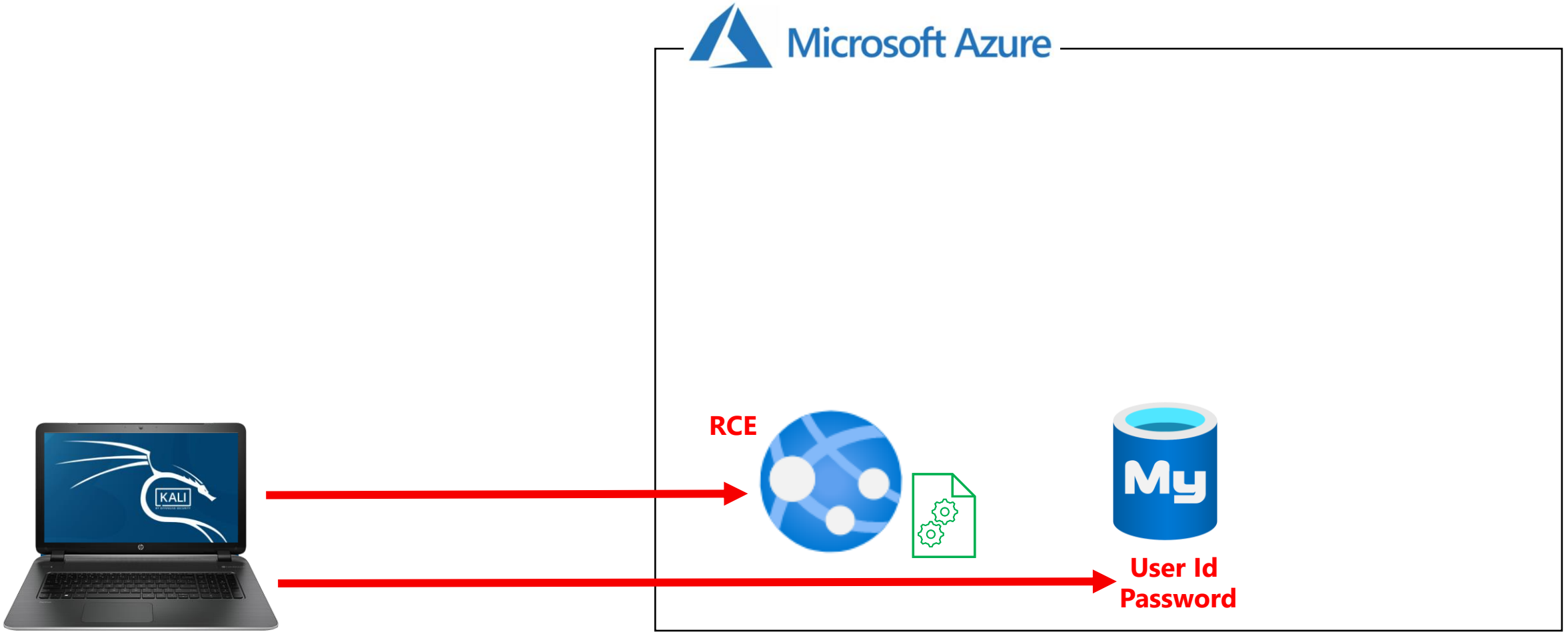


Azure Platform Attack Matrix

Recon	Exploitation	Initial Access	Credential Theft	Privilege Escalation	Persistence	Impact
Cloud provider IP range network scan	Remote code execution	Exposed cloud account credentials	Source control service scans	Privileged EC2 instances	Account manipulation	Azure Storage Dump
Cloud provider IP range vulnerability scan	Password Brute Force Attack	Insecure cloud account credentials	DevOps tools scans	Cloud Shell Privilege Escalation	Create account	Azure Disk Snapshot and Download
Cloud Service Discovery		Application vulnerability exploit	Credentials in configuration settings or files		Implant container image	Data destruction
		Compromised container images	Managed identity token theft		Network Security Group Backdoor	Resource hijacking
		Stolen cloud account credentials	Azure Blob/File Scan		Backdoor Azure function	Crypto-mining
		Dependency/Plugin vulnerability exploit	Harvesting connection strings			Denial of service
			Harvesting API keys			

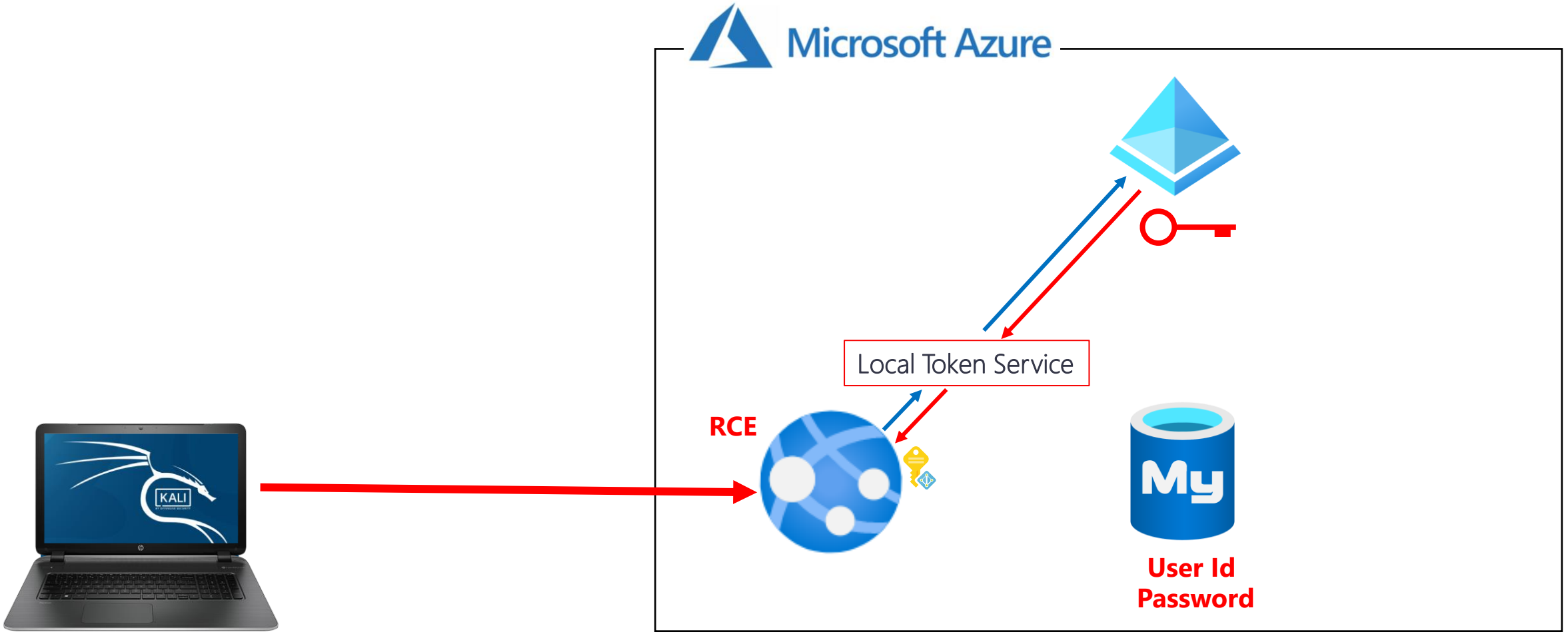
AZURE HANGOUT

Attack Scenario - DEMO



AZURE HANGOUT

Attack Scenario - DEMO



Azure Management API

- Azure control plane API Endpoint: management.azure.com
- Interacting with the API only requires a valid token issued to an authenticated entity

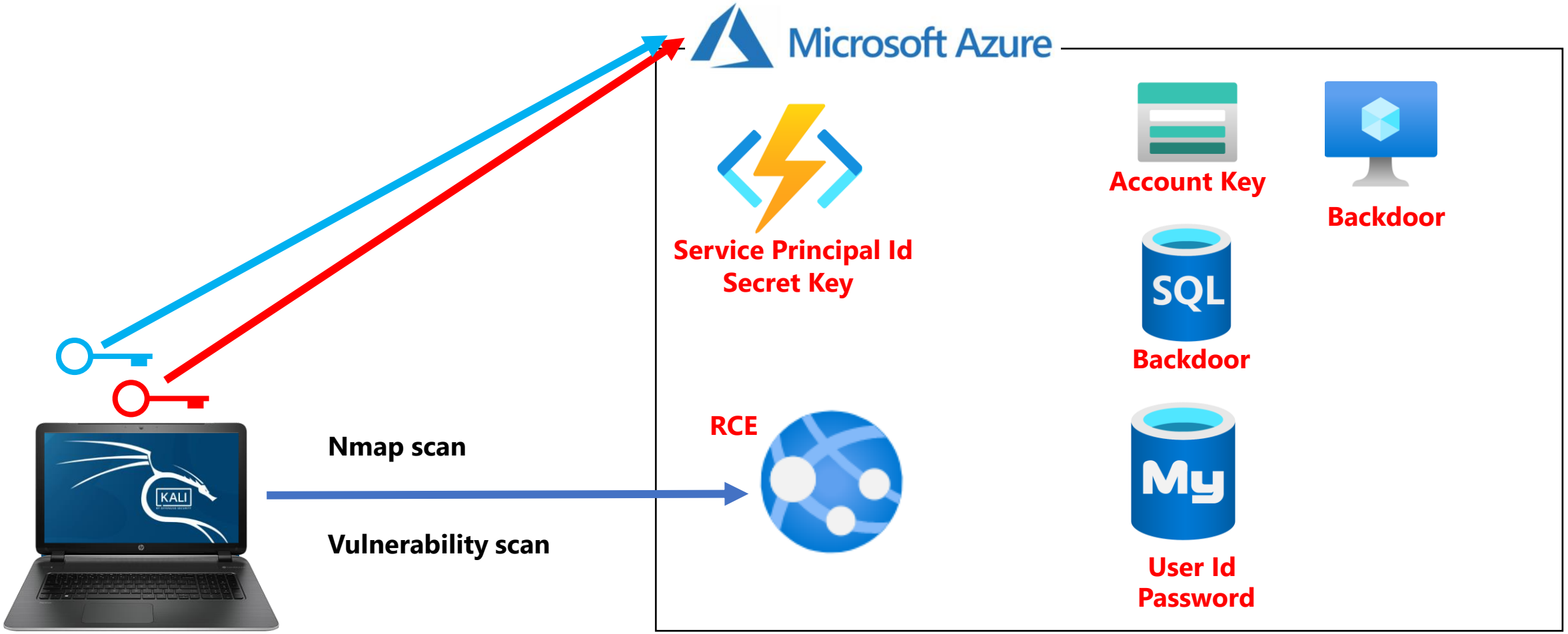
```
# API request format
{URI-scheme} :// {URI-host} / {resource-path} ? {query-string}

# Get a list of subscriptions
curl --header "Authorization: Bearer ${TOKEN}" \
https://management.azure.com/subscriptions?api-version=2020-01-01 | jq

# Get a list of resource groups for a subscription
curl --header "Authorization: Bearer ${TOKEN}" \
https://management.azure.com/subscriptions/${SUB_ID}/resourcegroups?api-
version=2019-10-01
```

AZURE HANGOUT

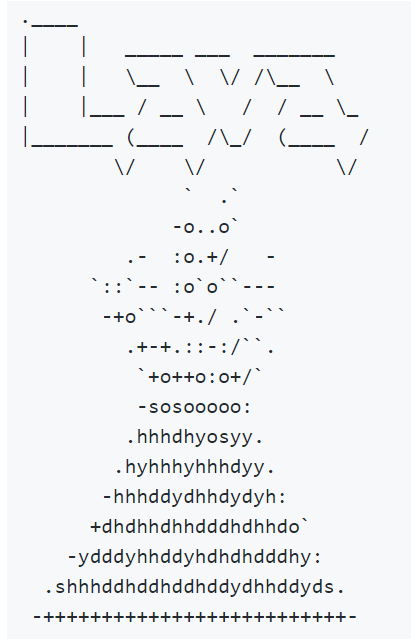
Attack Scenario - DEMO



AZURE HANGOUT

Lava - A Microsoft Azure exploitation framework

- A Microsoft Azure exploitation framework inspired by Pacu for AWS
- Contains multiple exploitation modules for pentesting Azure environments
  - `Azure AD`
  - `VM/VMSS`
  - `Storage Account`
  - `SQL Database`
  - `Privilege Escalation`
  - `Network`
  - `Persistence`
  - `Data Exfiltration`
- Creator: Matt Rottlevi
- Twitter: @mattrotlevi
- GitHub Repository: https://github.com/mattrotlevi/lava



AZURE HANGOUT

How to PREVENT? – Initial Access

- In the initial access phase a remote code execution vulnerability in an environment plugin was exploited
- Application and system vulnerabilities are still one of the MAIN entry vectors to environments
- Vulnerability assessment from development to production
  - CICD: Static code analysis; OSS Vulnerability; Passive Pen Test; Active Pen Test
- Use a Web Application Firewall
  - Application Gateway + WAF
  - Azure Frontdoor + WAF
- VM vulnerability assessment (Security Center Standard using Qualys)
- Container image vulnerability assessment (Security Center Standard using Qualys)

How to PREVENT? – Credential Theft and DB Access

- After initial access, we dumped the configuration settings and found credentials to access a database
- Credential Hotspots
  - DevOps tools (Azure DevOps variables; Jenkins)
  - Azure App Service Configuration Settings
  - Azure Function Configuration Settings
  - Automation account variables
  - Resource manager deployment outputs
- Enforce secret management
  - ARM Template Test Toolkit (ARM-TTK)
  - Use Azure Key Vault for ALL secrets

Azure Key Vault Referencing

- Referencing keys, secrets and certificates in Key Vault

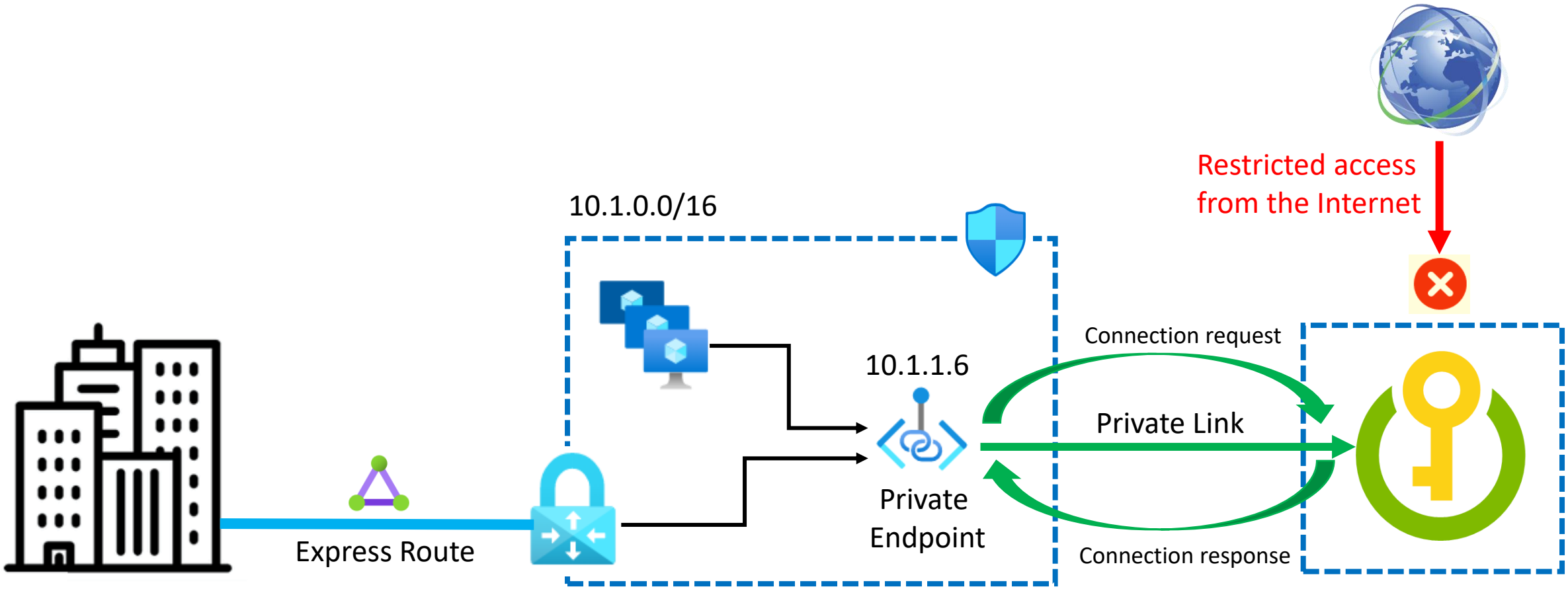
```
@Microsoft.KeyVault(SecretUri=https://myvault.vault.azure.net/secrets/mysecret/
ec96f02080254f109c51a1f14cdb1931)
```

- Alternatively

```
@Microsoft.KeyVault(VaultName=myvault;SecretName=mysecret;SecretVersion=ec96f02
080254f109c51a1f14cdb1931)
```

How to PREVENT? – Credential Theft and DB Access

- We were able to access the database directly from the Internet
- Use service firewall rules together with private endpoint (where possible)



How to PREVENT? – Credential Theft and Impact

- We used the stolen token from the managed identity to explore the environment
- Follow the principle of least privilege always
  - Only give permissions to resources that is needed
  - Even read-only permissions are dangerous
- Have a security baseline for every service that you adopt
  - Evaluate services, come up with best practices that fits into your security framework
  - Enforce governance at an organization level using Azure Policy

David Okeyode

THANK YOU!

Q and A???

- BLOG: https://azurehangout.com

asegunlolu

@asegunlolu