David Okeyode (MVP)

EMEA Chief Technology Officer for Azure at Palo Alto Networks

Bio: Over a decade of experience in Cybersecurity (consultancy, design, implementation) with organizations of different sizes from start-ups to major enterprises to government organizations. Authored two books on Azure security - "Penetration Testing Azure for Ethical Hackers" and "Microsoft Azure Security Technologies Certification and Beyond" (https://amzn.to/3C7mrcL). Also authored multiple cloud computing courses for the popular cybersecurity training platform - Cybrary. Holds over 15 cloud certifications across Azure and AWS platforms, including the Azure Security Engineer, Azure DevOps and AWS Security Specialist certifications.

@asegunlolu

http://www.youtube.com/c/DavidOkeyode

http://azurehangout.com

Microsoft® Most Valuable Professional

Microsoft Certified Azure AI Engineer Associate

Microsoft Certified Azure Developer Associate

Microsoft Certified Azure Administrator Associate

Microsoft Certified Azure Security Engineer Associate

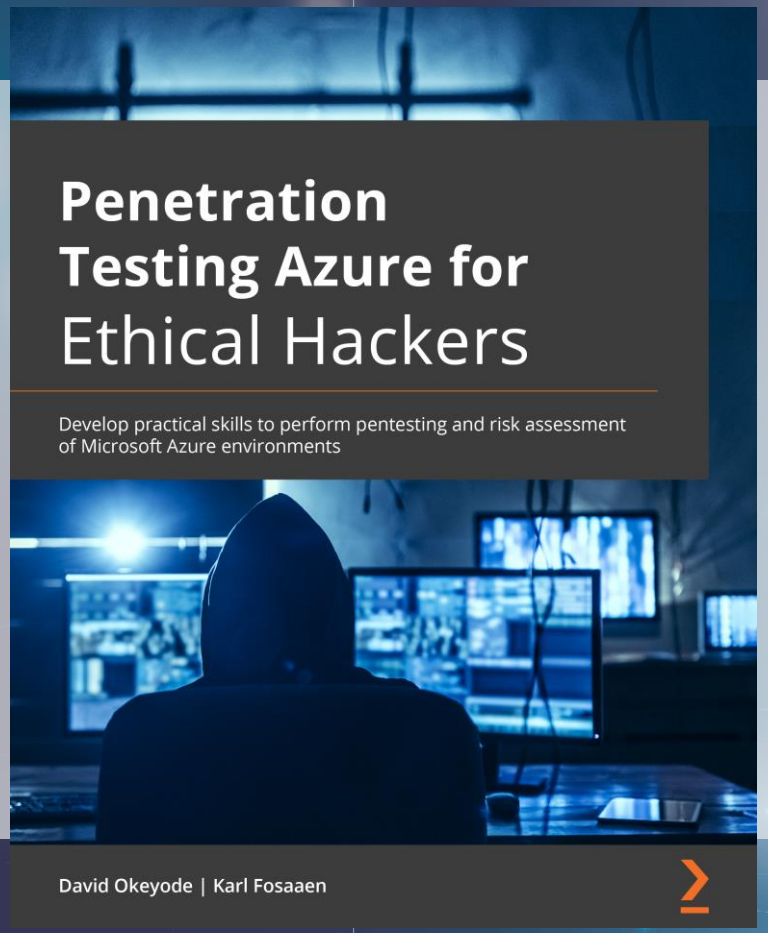
Microsoft Certified Azure Solutions Architect Expert

Microsoft Certified Azure DevOps Engineer Expert

aws certified Solutions Architect Professional

aws certified Security Specialty

Available for order on Amazon



✔ Identify how administrators misconfigure Azure services, leaving them open to exploitation

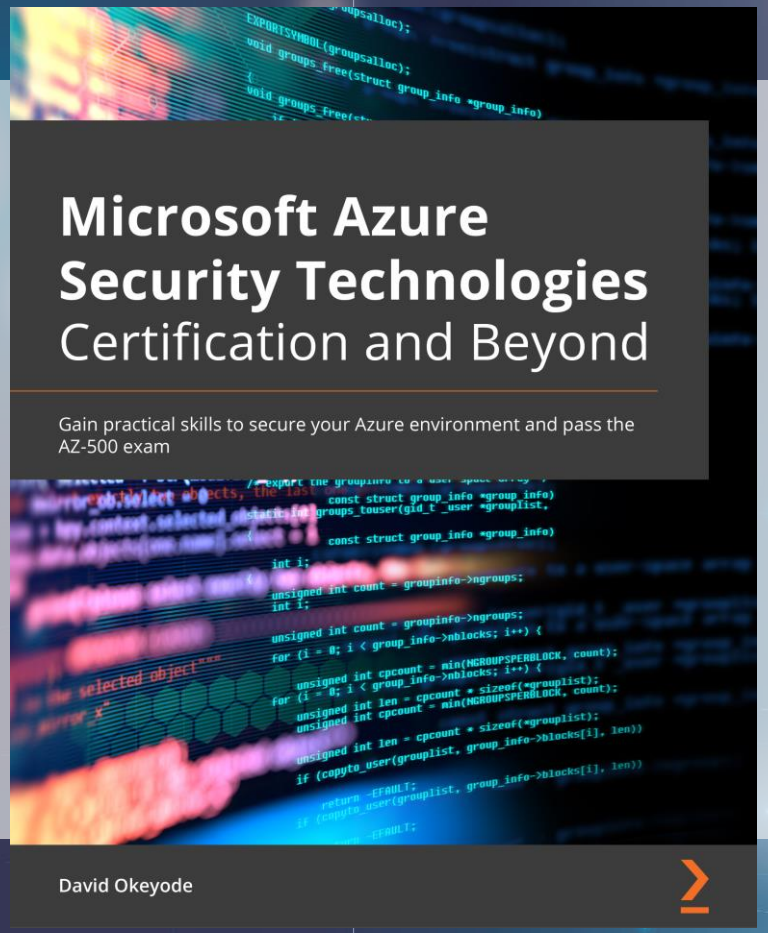
✔ Explore processes and techniques for exploiting Azure security issues

✔ Discover various tools and techniques to perform successful penetration tests on your Azure infrastructure

Amazon URL: https://amzn.to/2Vt0Jjx

Packt

Available for order on Amazon



✔Develop practical skills to protect your organization from constantly evolving cloud security threats

✔Hands-on easy to follow practices on securing identities, networks, hosts, containers, storage and databases in Azure

✔Become well-versed with the AZ500 exam objectives with the help of practice questions

Amazon URL: https://amzn.to/2VOD11z

Packt

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

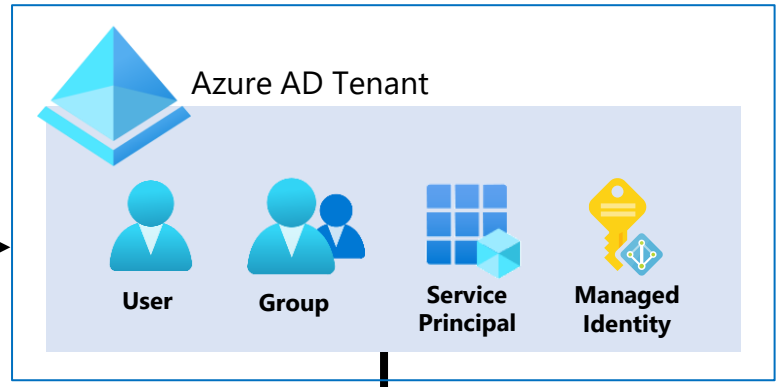
What is a vulnerability?

- A weakness in a system that can be exploited by an attacker to deliver a successful attack
- Software Flaws
  - Unintended functionality
  - Zero days or publicly reported
- Feature misuse
  - Intended functionality
- User error OR misconfiguration

AZURE HANGOUT

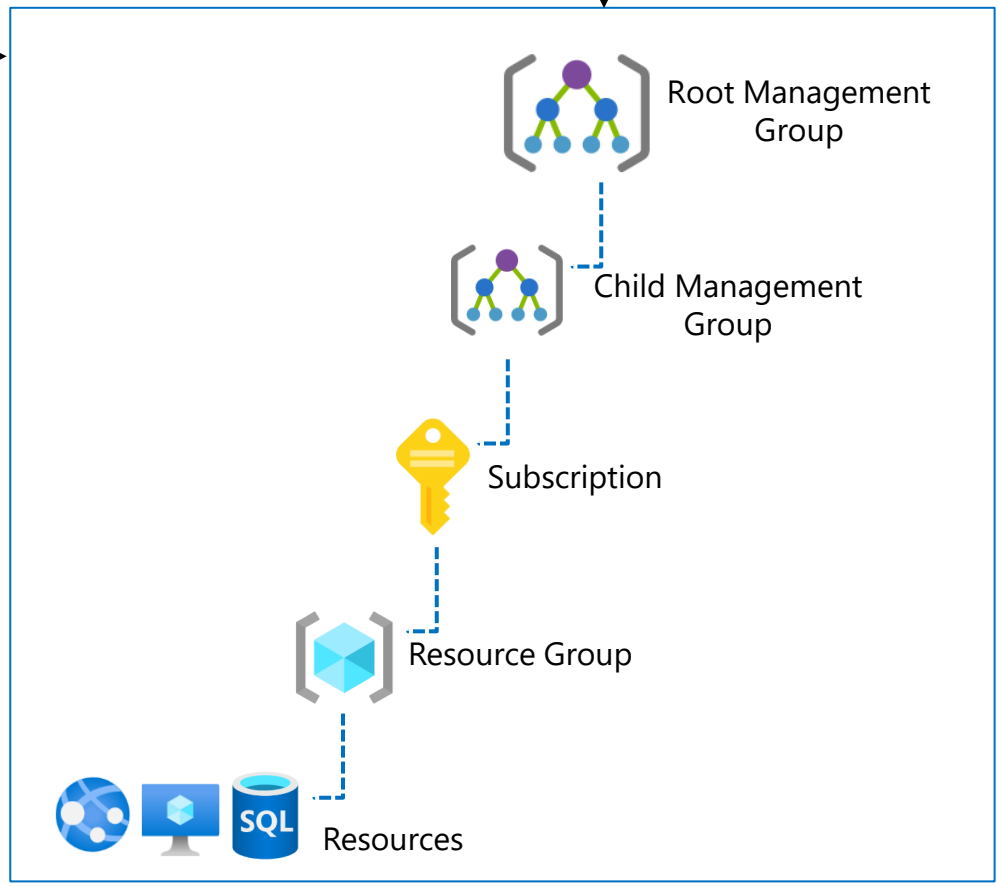
Azure Organization Structure

Azure AD roles are used to grant access to Azure AD. Example roles are,
Global Administrator and User Administrator



Azure RBAC roles are used to grant access to Azure resources. Example roles are,
Owner, Contributor and Reader

```
"permissions": [
   {
     "actions": [ ],
     "notActions": [ ],
     "dataActions": [ ],
     "notDataActions": [ ]
   }
 ],
```



Azure RBAC - https://azure.permissions.cloud

317

BUILT-IN ROLES

Number of built-in roles provided by Azure.

13,440

ACTIONS

Number of known actions within the Azure RBAC service.

13,440

API METHODS

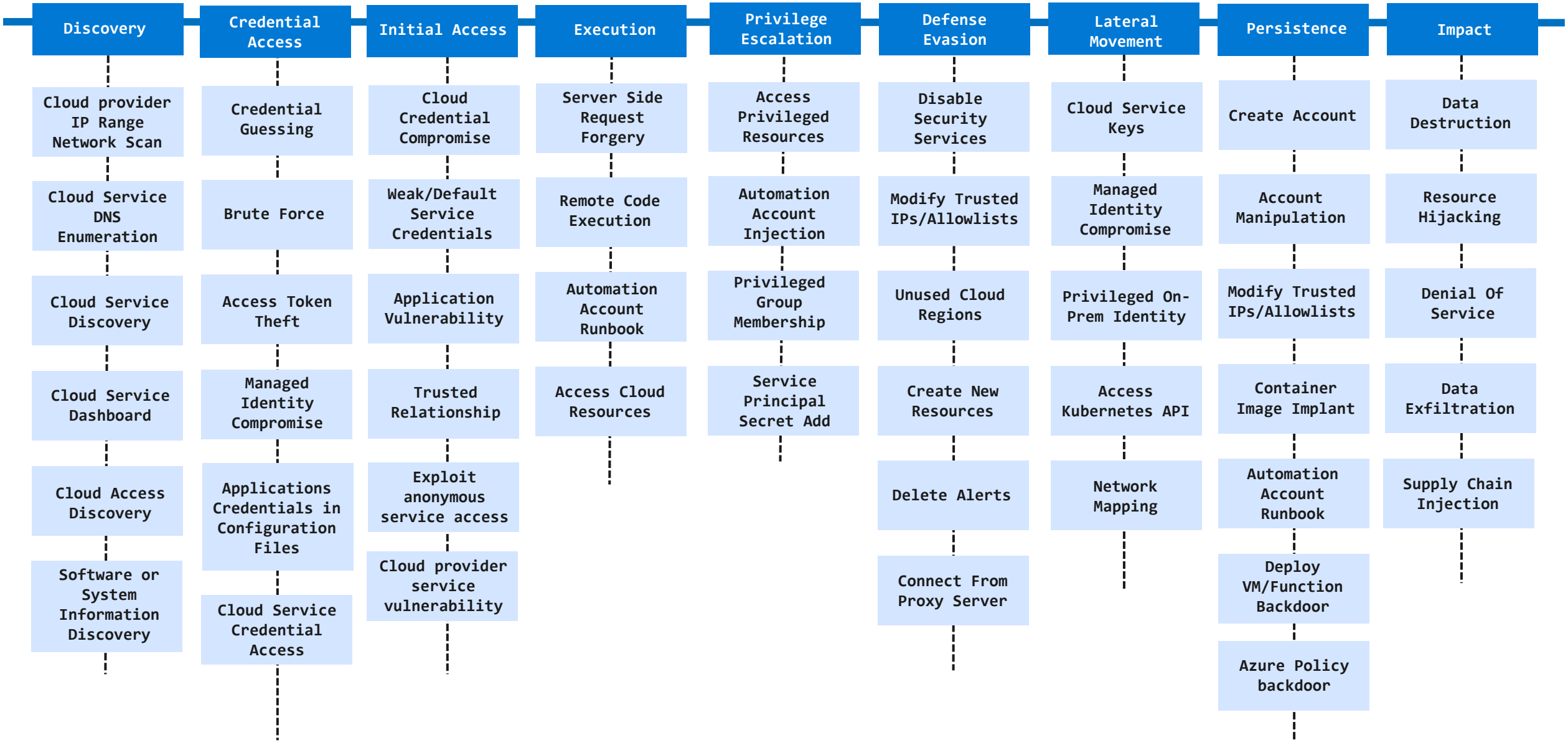
Number of known API methods within all of Azure.

MITRE ATT&CK® Matrix for IaaS

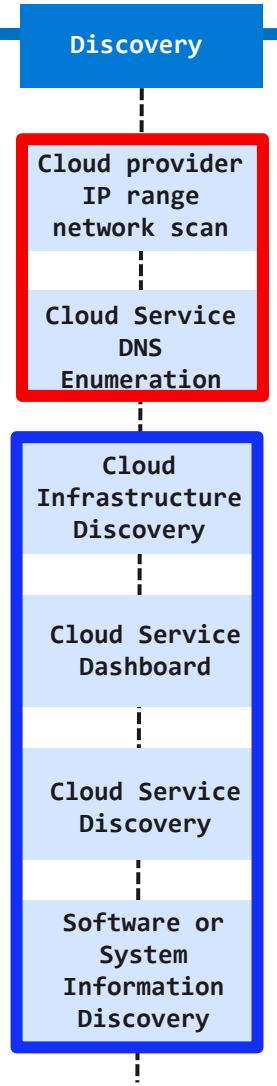
- Globally-accessible knowledge base of adversary tactics and techniques and procedures
- https://bit.ly/mitreazure

Azure Attack Matrix

davidokeyode.medium.com



Discovery



- Unauthenticated Discovery
  - Cloud provider IP range network scan
  - Cloud Service DNS Enumeration
- Authenticated Discovery
  - Cloud Infrastructure Discovery
  - Cloud Service Discovery

Unauthenticated Discovery – Cloud Provider IP Range Scan

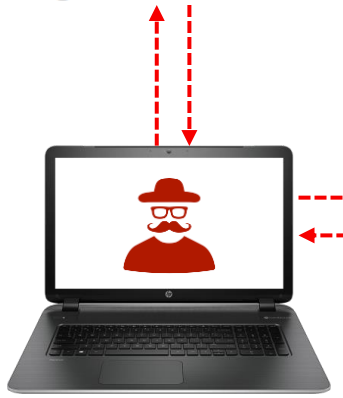
- Discovery
- **Cloud provider IP range network scan**
- Cloud Service DNS Enumeration
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Software or System Information Discovery

Azure IP Ranges and Service Tags – Public Cloud

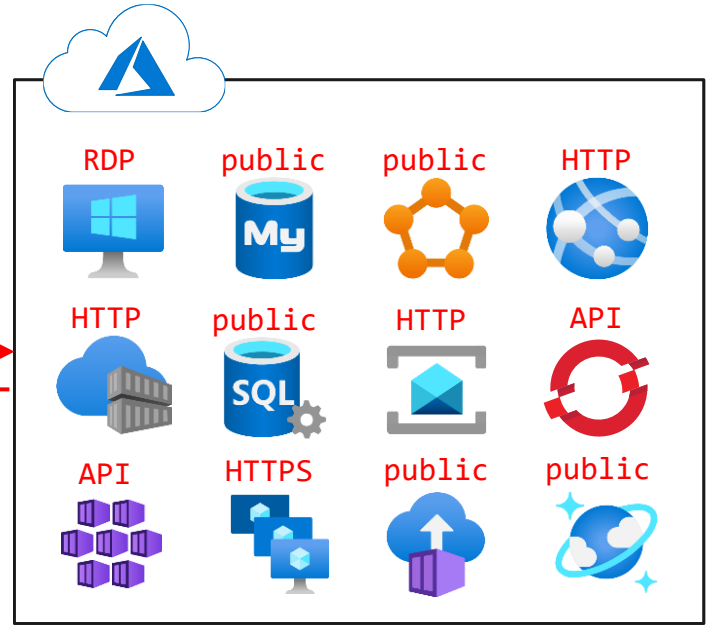
Important! Selecting a language below will dynamically change the complete page content to that language.

Language: English Download

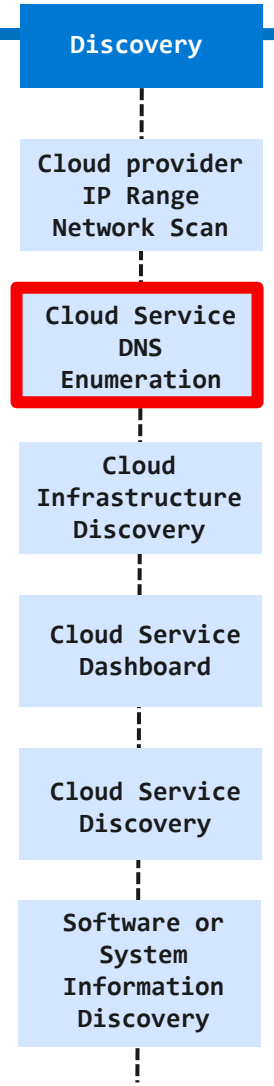
Azure IP Ranges and Service Tags – Public Cloud



Azure_Public_IP_Range.json



Unauthenticated Discovery – Cloud Service DNS Enumeration



<resource instance name>.<service dns suffix>

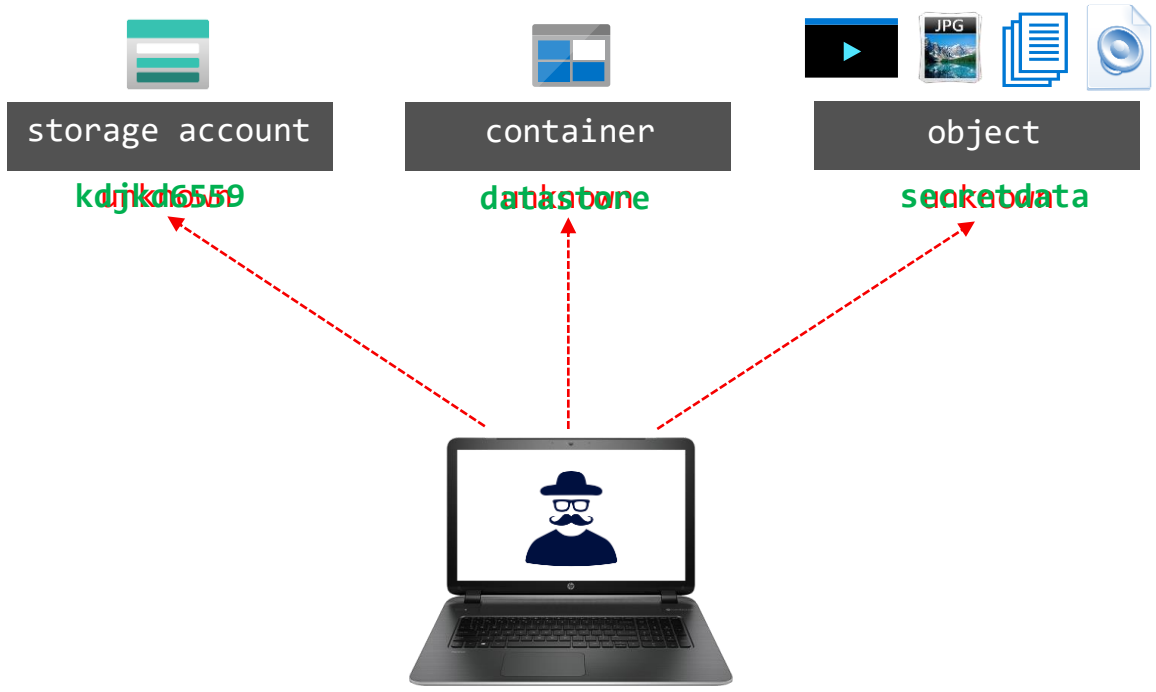
azureoffensive.blob.core.windows.net

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	Azure Cache for 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

Discovery – Cloud Service DNS Enumeration

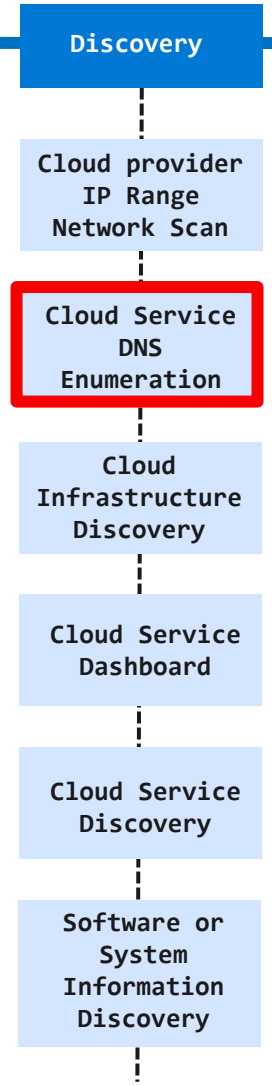
- Discovery
- Cloud provider IP Range Network Scan
- **Cloud Service DNS Brute Enumaration**
- Cloud Service Discovery
- Cloud Service Dashboard
- Cloud Access Discovery
- Software or System Information Discovery

- The subdomain and domain name forms an *endpoint*
  - Blob service: http://*mystorageaccount*.blob.core.windows.net/*<container>*/*<object>*
  - Permission can be configured to allow anonymous access on the container level
  - Blob access OR container access



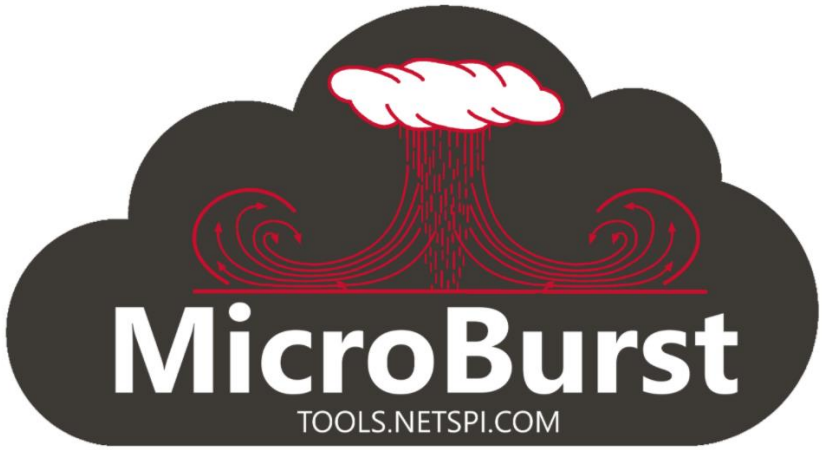
http://mystorageaccount.blob.core.windows.net/<container>/<object>

Discovery – Cloud Service DNS Enumeration (Tools)



- DNScan
  - Description: Python wordlist-based DNS subdomain scanner
  - Creator: rbsec
  - Open Source or Commercial: Open source project
  - GitHub Repository: https://github.com/rbsec/dnscan
  - Language: Python
- GoBuster
  - Description: Tool used to brute-force DNS subdomains
  - Creator: OJ Reeves (Twitter: @TheColonial)
  - GitHub: https://github.com/OJ/gobuster/
  - Language: Go
- cloud_enum
  - Description: Multi-cloud OSINT tool to enumerate public resources in AWS, Azure, and Google Cloud.
  - Creator: (Twitter: @init_string)
  - GitHub: https://github.com/initstring/cloud_enum
  - Language: Python

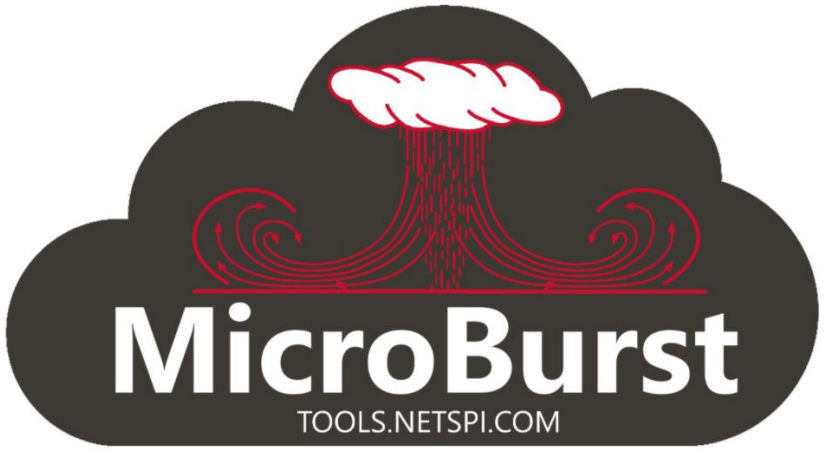
MicroBurst Overview



- A group of PowerShell scripts that can be used for different attacks in Azure
- Includes a script for Azure cloud service DNS enumeration
- **Creator**: Karl Fosaaen (**Twitter**: @kfosaaen)
- **GitHub Repository**: https://github.com/NetSPI/MicroBurst
- **Open Source or Commercial**: Open-source project
- **Language**: PowerShell

DEMO

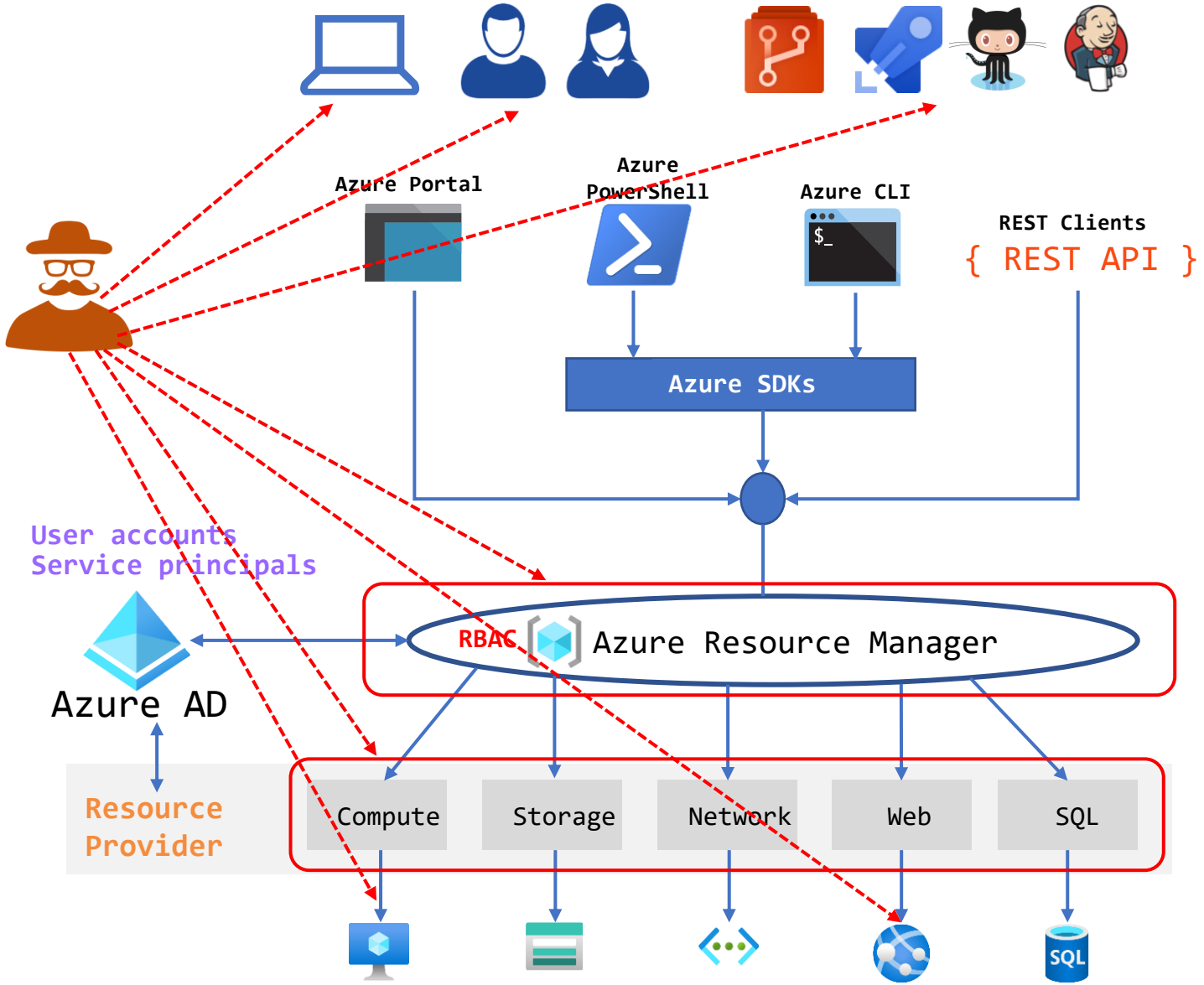
Using MicroBurst For Anonymous Enumeration and Access



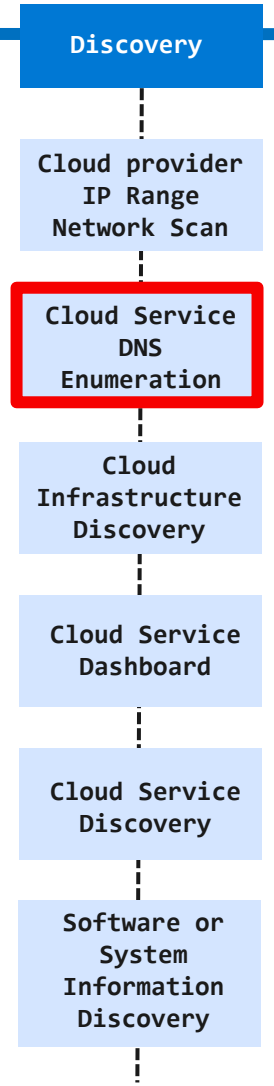
Initial Access – Cloud Credential Compromise

- Initial Access
- **Cloud Credential Compromise**
- Weak Service Credentials
- Application Vulnerability
- Trusted Relationship
- Bash/CMD inside container

- Targets
  - Azure AD user account
  - Azure AD service principal
  - Azure AD issued access token
- Compromise methods
  - Target users/admins
  - DevOps systems
    - Source Control
    - CICD Tools
  - Admin workstations
  - Azure hosted apps



Discovery – Cloud Service DNS Enumeration

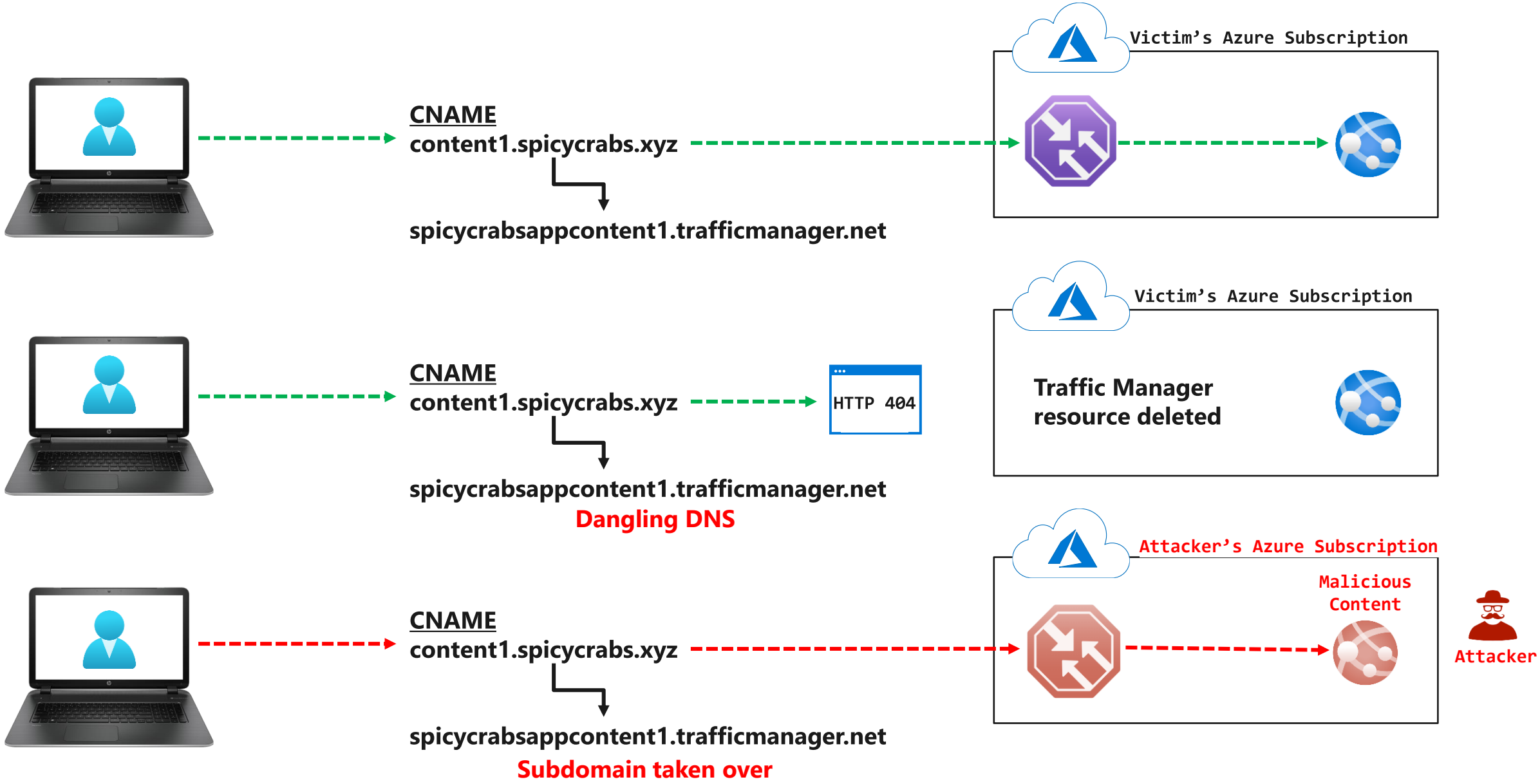


<resource instance name>.<service dns suffix>

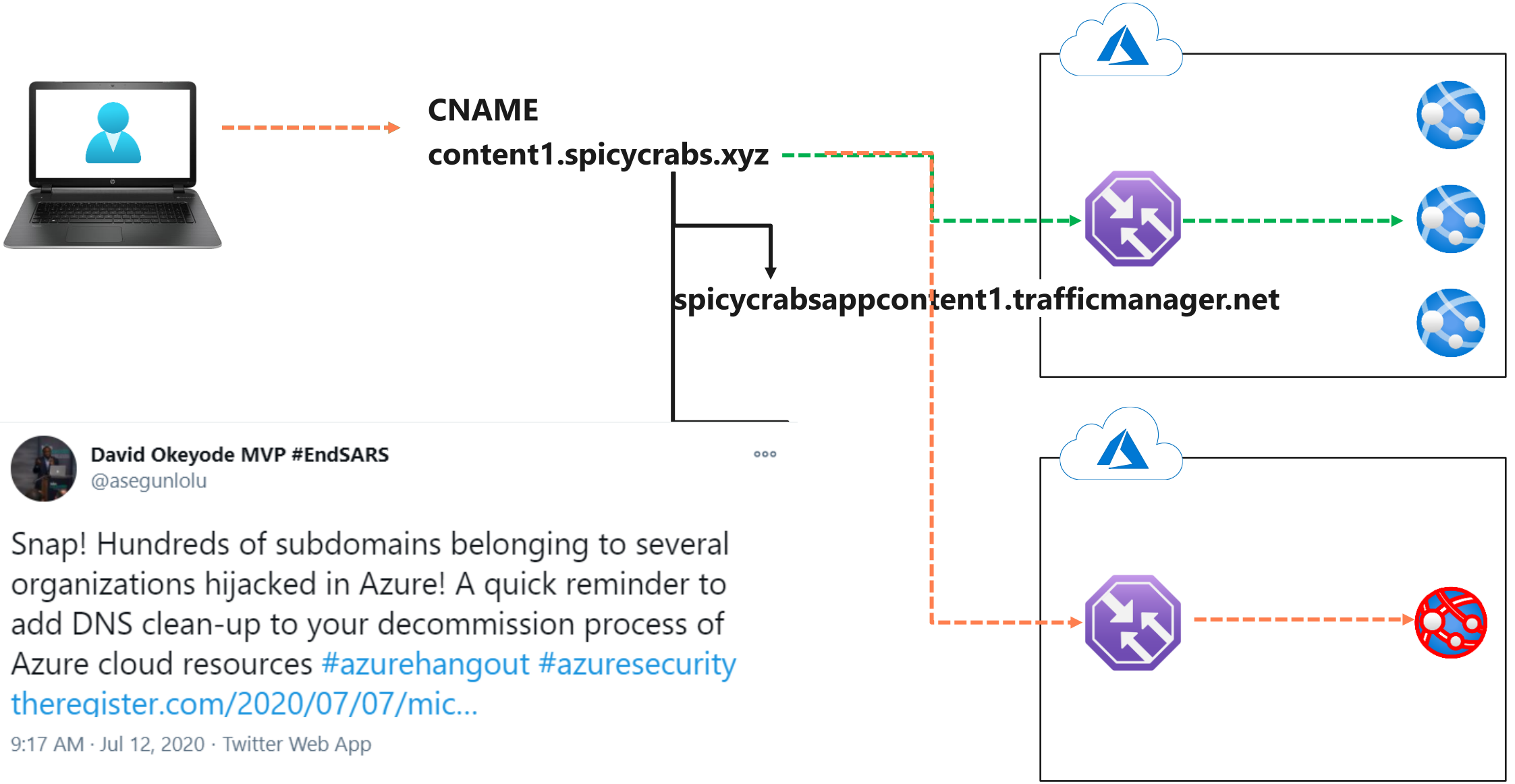
azureoffensive.blob.core.windows.net

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	Azure Cache for Redis
documents.azure.com	Databases-Cosmos DB
database.windows.net	Databases-MSSQL
vault.azure.net	Key Vaults
azureedge.net	CDN
azurecr.io	Container Registry
servicebus.windows.net	Service Bus and Event Hub

Discovery Techniques – Subdomain Takeover



Discovery Techniques – Subdomain Takeover



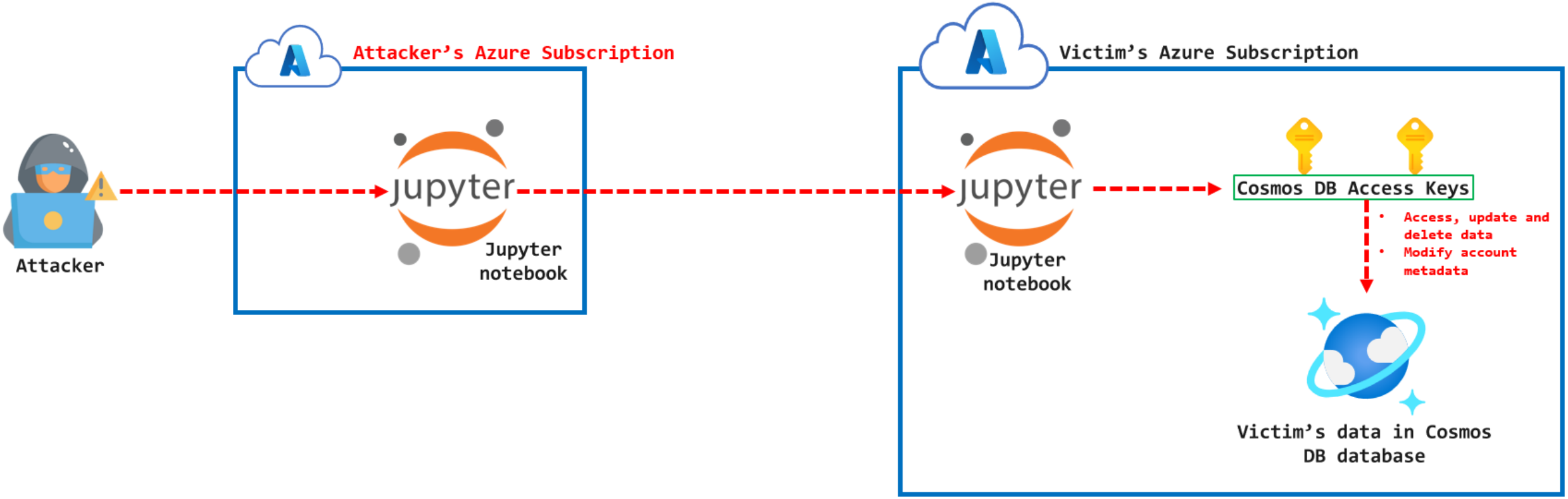
David Okeyode MVP #EndSARS
@asegunlolu

Snap! Hundreds of subdomains belonging to several organizations hijacked in Azure! A quick reminder to add DNS clean-up to your decommission process of Azure cloud resources #azurehangout #azuresecurity theregister.com/2020/07/07/mic...

9:17 AM · Jul 12, 2020 · Twitter Web App

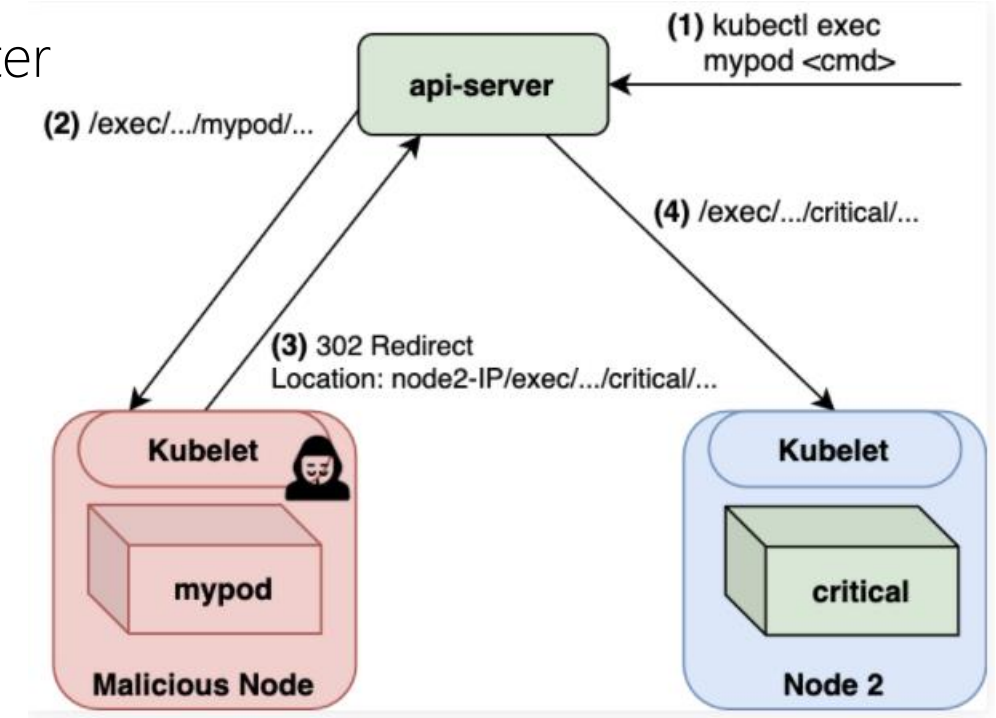
ChaosDB

- Platform database (CosmosDB) feature (Jupyter notebook) exploited
- C# code ran as root
- Exploited to remove block rules in iptables
- Recon exposed certificates later used to access internal systems
- Exposed database access keys for thousands of users



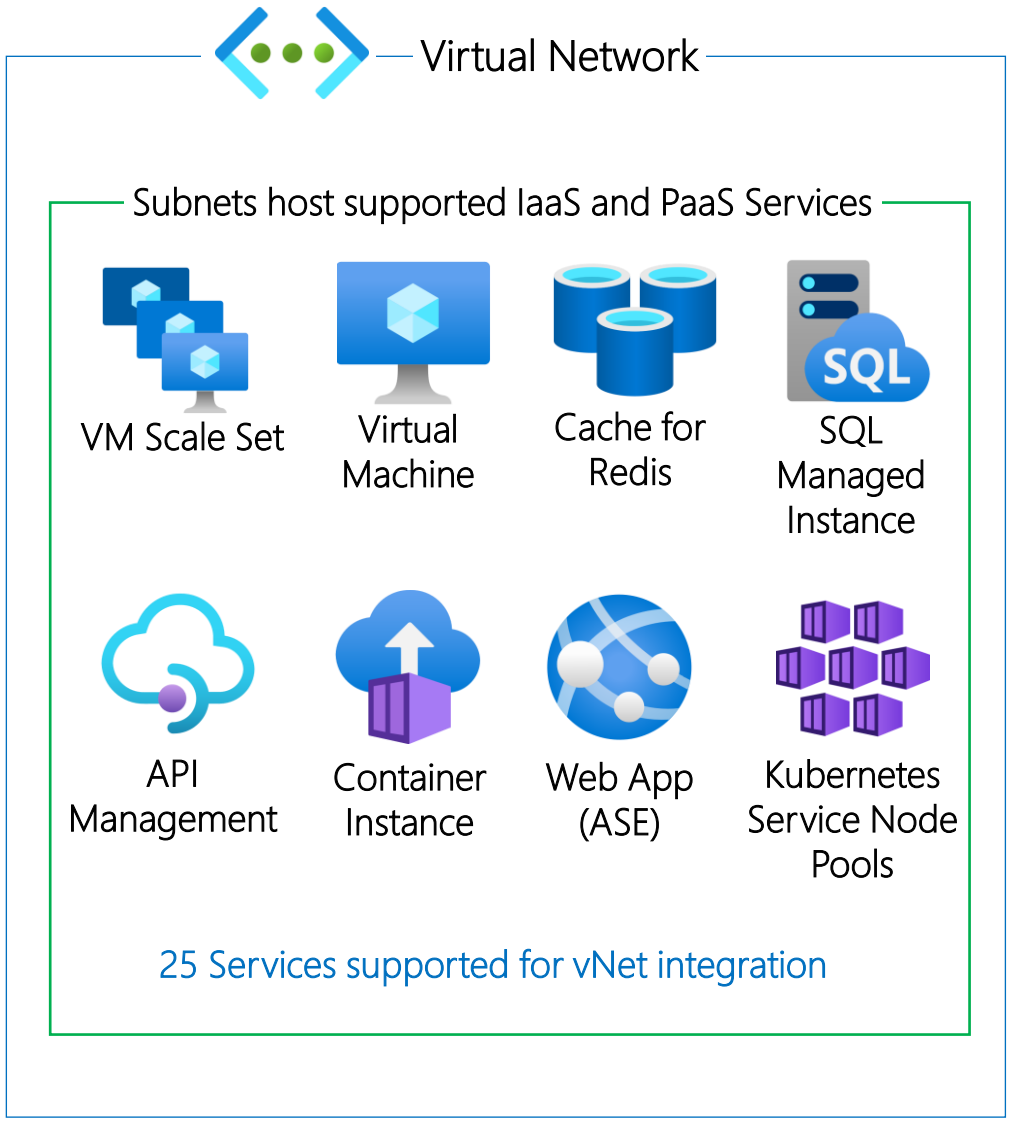
Azurescape

- Vulnerability in container-as-a-service solution – Container instance
- Researcher used “whoC” to enumerate the underlying container runtime information
- Discovered outdated version of “runC”
- Exploit — CVE-2019–5736 to escape the container to the node
- Outdated K8s version detected
- Bridge pod tricked to expose privileged service token
- Compromise of other nodes and containers in the cluster



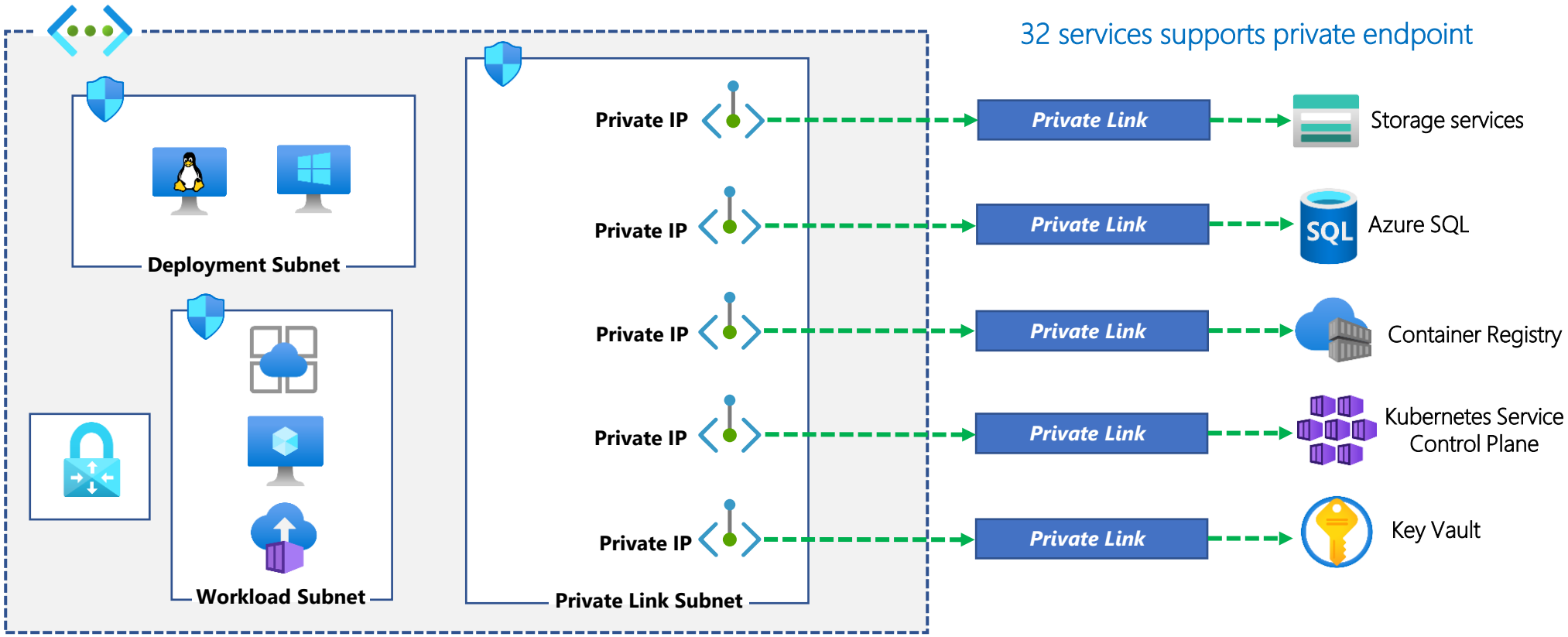
LESSON 1 – Normalize private network access for platform services

- vNet integration
  - Platform service deployed into a virtual network subnet
  - Ingress and egress traffic control
  - Supported by 23 platform-managed services
  - Dedicated subnet required by MOST services
  - Some services require *delegated access*



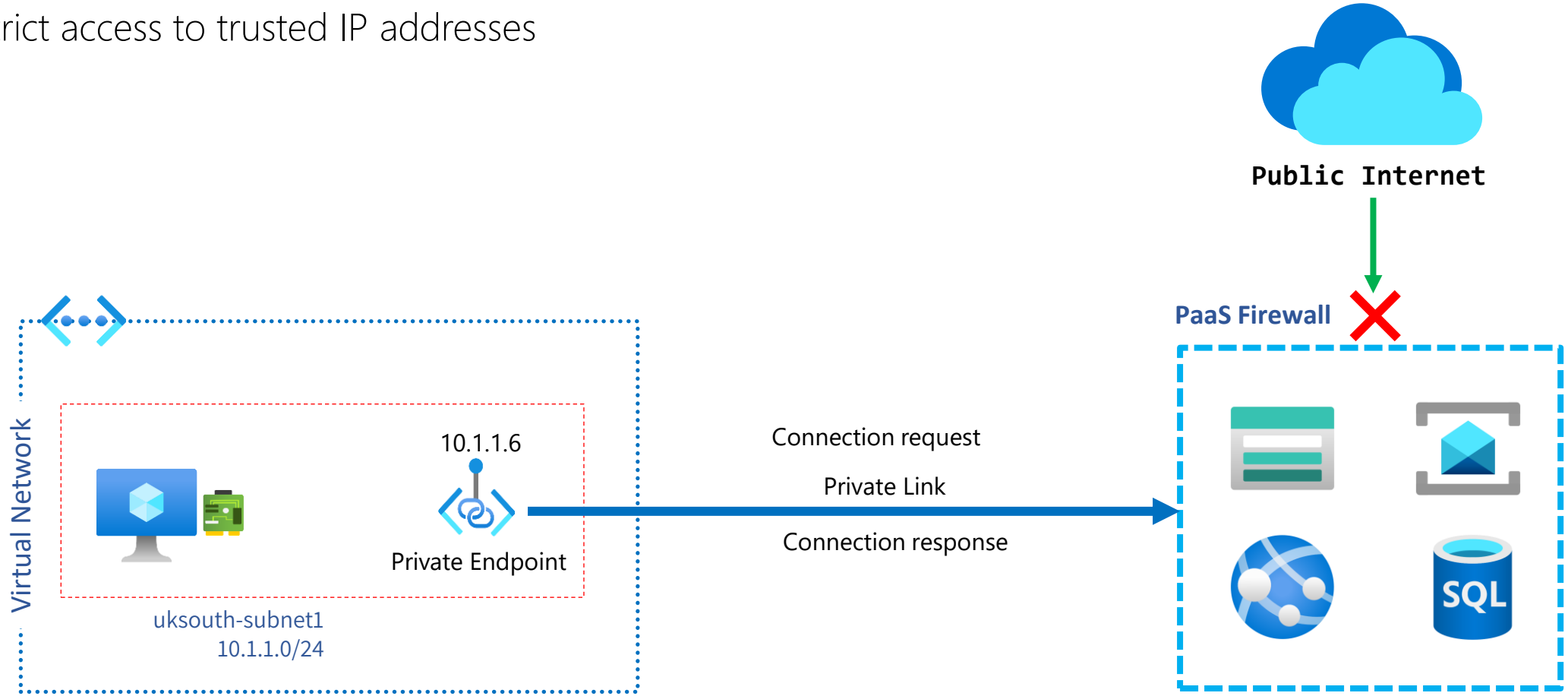
LESSON 1 - Normalize private network access for platform services

- Private endpoint
  - Link platform services to a private network
  - Ingress requests only



LESSON 1 - Normalize private network access for platform services

- Private endpoint
  - Link platform services to a private network
  - Ingress requests only
- Service firewall
  - Restrict access to trusted IP addresses

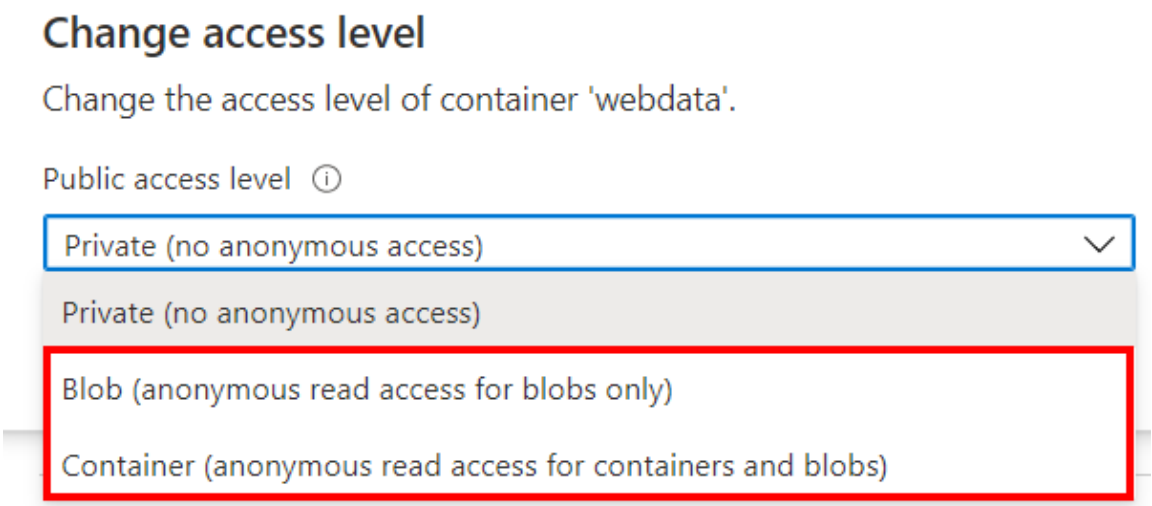


LESSON 2 – Disable key-based and local authentication where possible

- Anonymous
- Key based authentication
  - Long lived or temporary access tokens
- Identity-based authentication
  - Local authentication
  - Azure Active Directory or Active Directory

Anonymous access

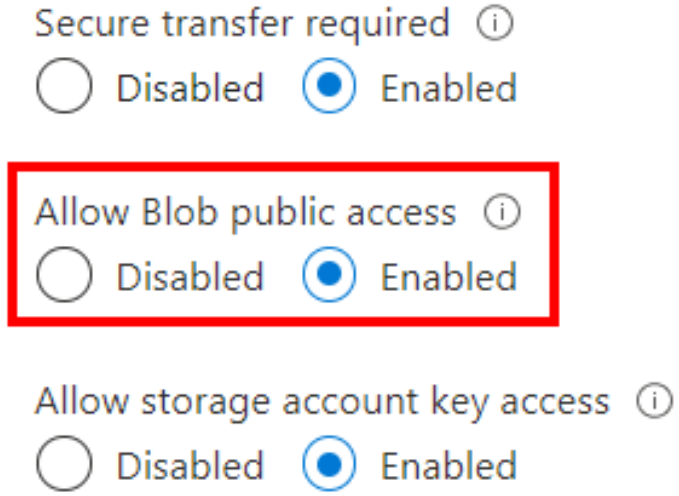
- Azure Blob Storage Container
- Azure Container Registry
- Information needed for external attack
  - Resource name
  - Container and/or object name for blob service
  - Repository and image name for container registry



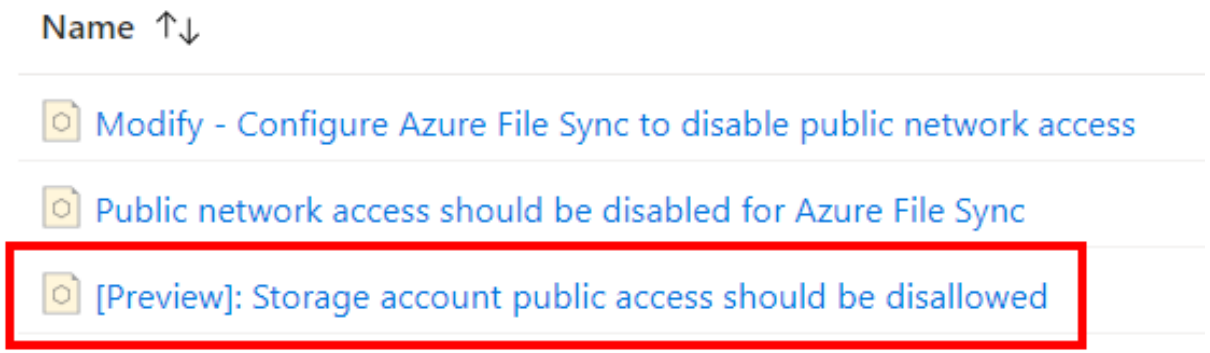

```
david_okeyode@Azure:~$ az acr show -n doacr3585
{
  "adminUserEnabled": false,
  "anonymousPullEnabled": true,
  "creationDate": "2021-09-04T16:08:17.588073+00:00",
  "dataEndpointEnabled": false,
  "dataEndpointHostNames": [],
  "encryption": {
    "keyVaultProperties": null,
    "status": "disabled"
  },
```

Anonymous access

- Can be disabled per-resource
- Can be disabled centrally using Azure policy

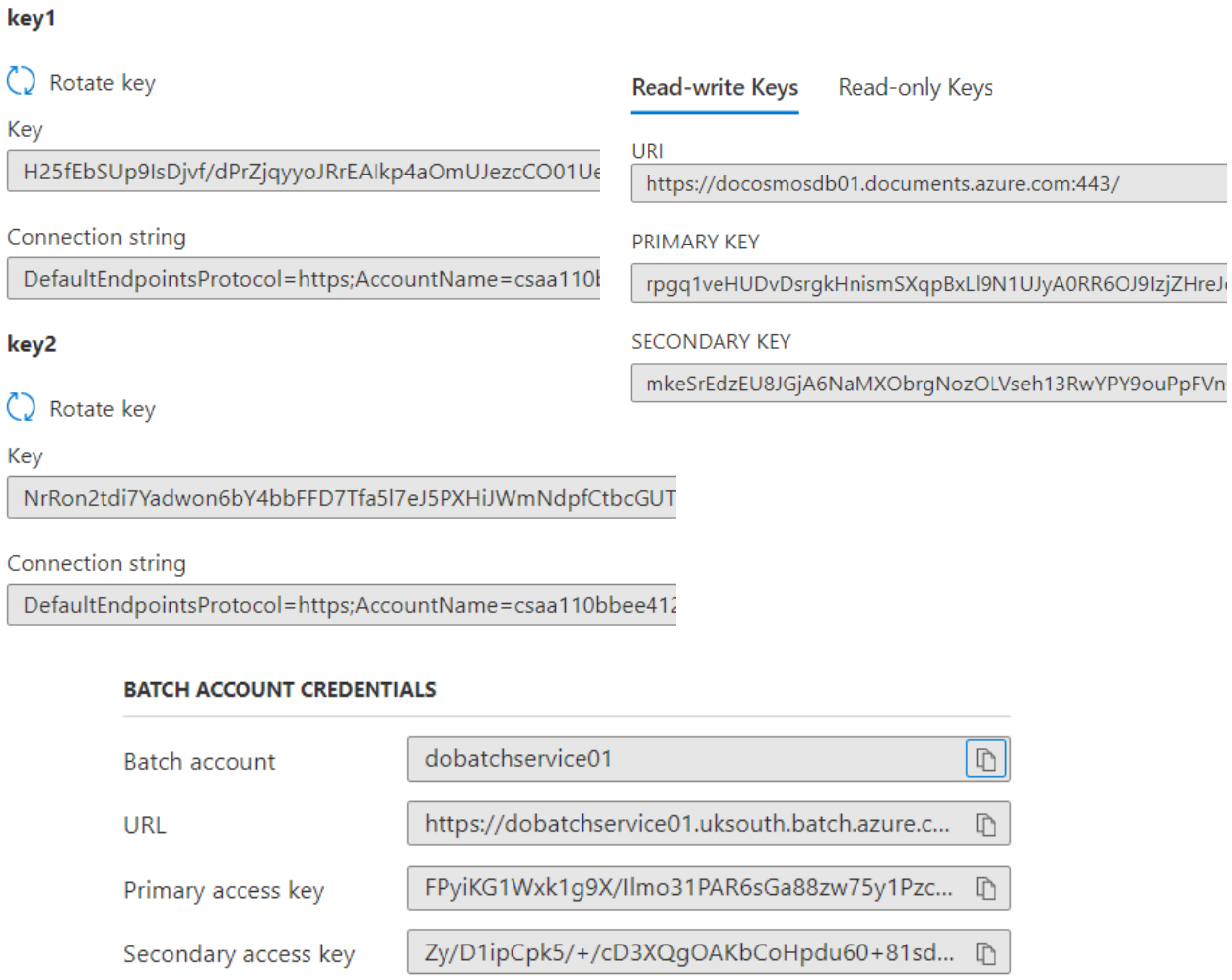



```
az acr update --name $ACR --anonymous-pull-enabled false
```



Long-lived access keys

- Supported by 28 services including:
  - Storage account; Cosmos DB
  - Batch accounts; Service Fabric Clusters; SignalR
  - Cognitive Service; Bot Service
  - Data Factory
  - App config
- Access level range:
  - Unrestricted management and/or data plane access
  - Read/write data plane permissions
  - Read-only data plane permissions

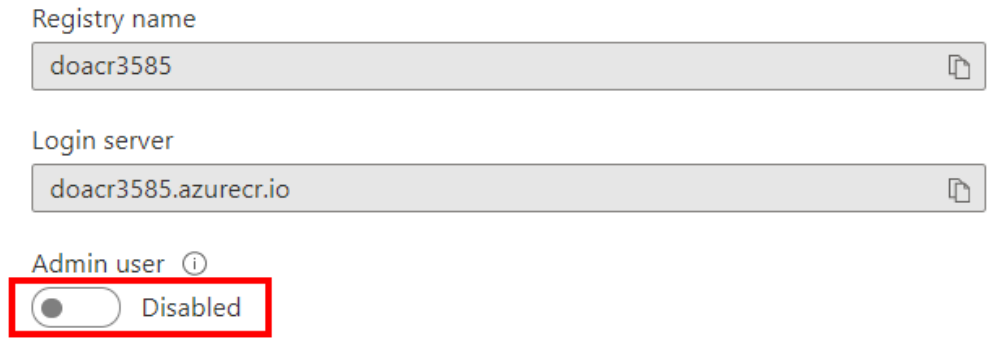


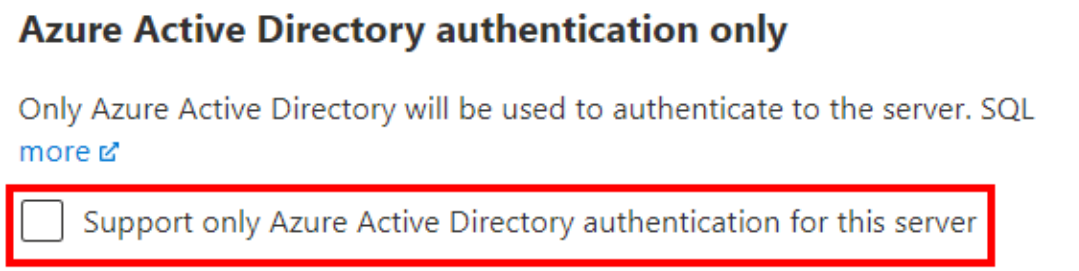
Long-lived access keys

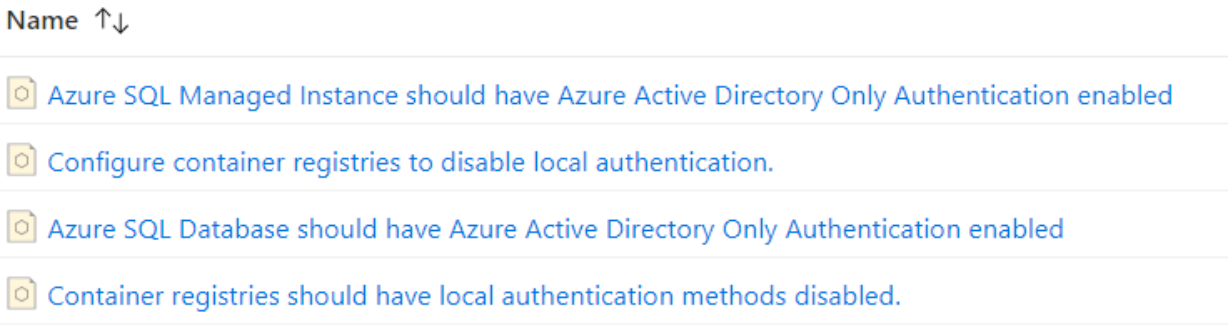
- Storage Account
  - Two 512bit access keys
  - Unrestricted data plane access for all account storage services
  - Permission: *Microsoft.Storage/storageAccounts/listkeys/action*
    - **Built-in Roles**: Owner, Contributor, Virtual Machine Contributor, Reader and Data Access, Storage Account Key Operator Service Role, Log Analytics Contributor, Logic App Contributor, DevTest Labs User, Disk Snapshot Contributor
    - **Custom Roles** with the permission
- Cosmos DB
  - Four access keys – two read/write keys; two read-only keys
  - Full control of Cosmos DB resources in a particular account
  - Permission: *Microsoft.Storage/storageAccounts/listkeys/action*
    - **Built-in Roles**: Owner, Contributor, Virtual Machine Contributor, Reader and Data Access, Storage Account Key Operator Service Role, Log Analytics Contributor, Logic App Contributor, DevTest Labs User, Disk Snapshot Contributor
    - **Custom Roles** with the permission

Local Authentication

- VMs and VM scale sets
- Azure SQL database and Azure SQL Managed Instance
- Azure Container Registry (ACR)
- Can be disabled for both Azure SQL, ACR
- Centrally enforced using Azure policy







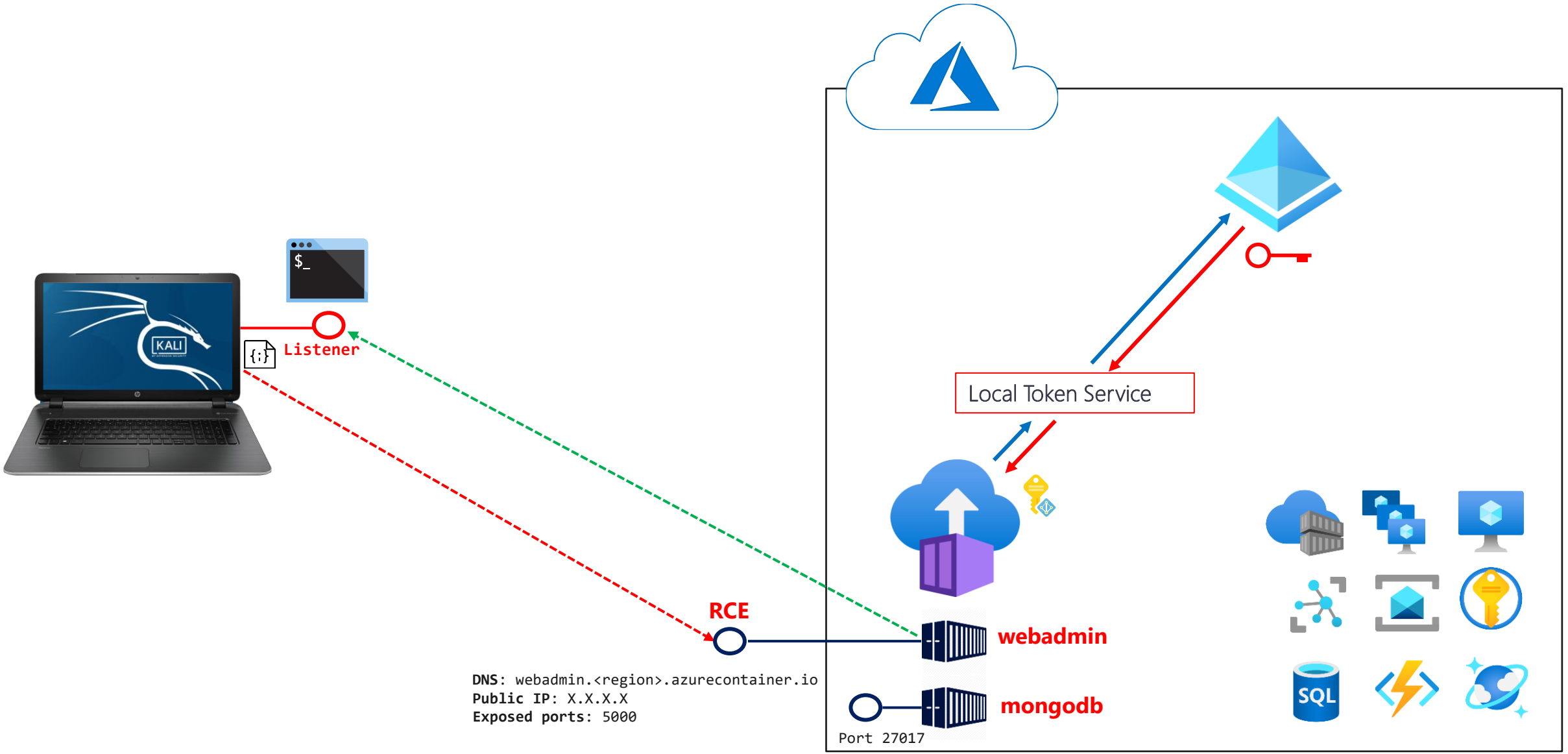
Best practices – Authentication and access methods

- Disable local auth, long-lived access keys, SAS generation where possible
  - Monitor configuration for status changes
  - Monitor events for usage (resource logs)
- Where not possible to disable, do the following:
  - Store in Key Vault
  - Regularly rotate
  - Enable private link/vNet integration as a second line of defense

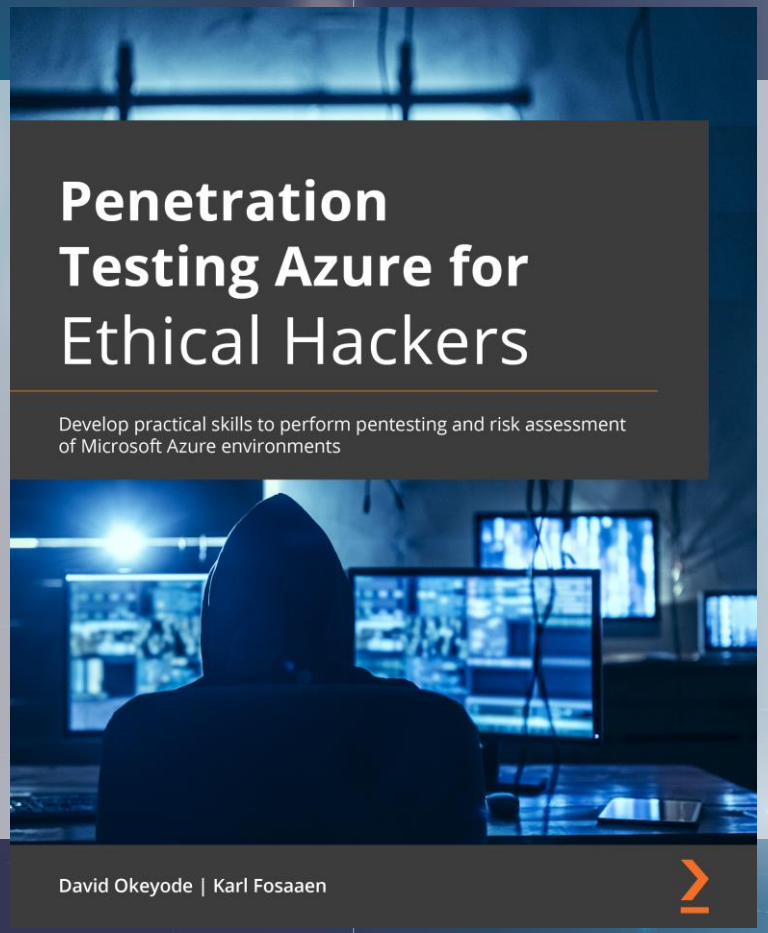
LESSON 3 – Runtime protection for platform compute services

- Ease, speed, reduced management cost VS visibility
- Embedded runtime protection as part of shift-left processes

DEMO - Exploiting Container Instance Workload



Available for order on Amazon



✔ Identify how administrators misconfigure Azure services, leaving them open to exploitation

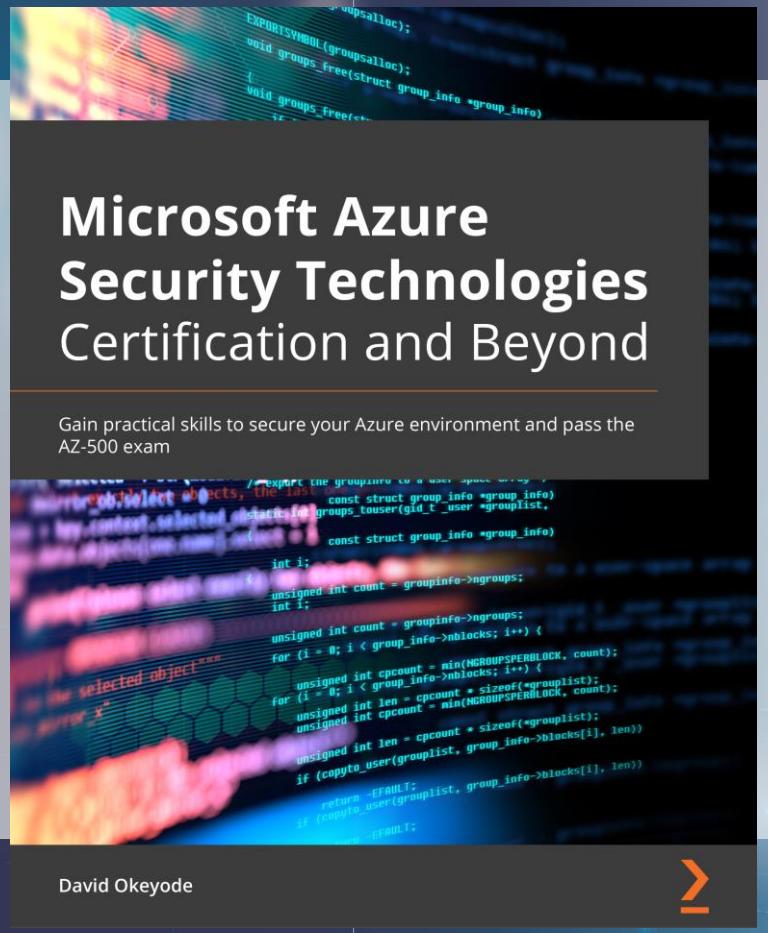
✔ Explore processes and techniques for exploiting Azure security issues

✔ Discover various tools and techniques to perform successful penetration tests on your Azure infrastructure

Amazon URL: https://amzn.to/2Vt0Jjx

Packt

Available for order on Amazon



✔Develop practical skills to protect your organization from constantly evolving cloud security threats

✔Hands-on easy to follow practices on securing identities, networks, hosts, containers, storage and databases in Azure

✔Become well-versed with the AZ500 exam objectives with the help of practice questions

Amazon URL: https://amzn.to/2VOD11z

Packt