Breaking Boundaries: Multi-Cloud Red Teaming Through Misconfigurations

@gr33nm0nk2802

Cloud Red Teaming Agenda

- Cloud 101
- Red Teaming 101
- IAM Concepts
- Cloud-Red-Labs Overview and Lab Safety.
- Azure Attack Flow and Practical Demonstrations
- AWS Attack Flow and Hands-On Demonstrations
- Detection and Mitigation Strategies
- Q&A Preparation

aws sts get-caller-identity

Syed Modassir Ali a.k.a **@gr33nm0nk2802**

Offensive Security Engineer. Red Teamer

Community Contributor.

Learn to build and break Stuffs.

https://linkedin.com/in/gr33nm0nk2802

Cloud 101

Cloud 101

Cloud 101

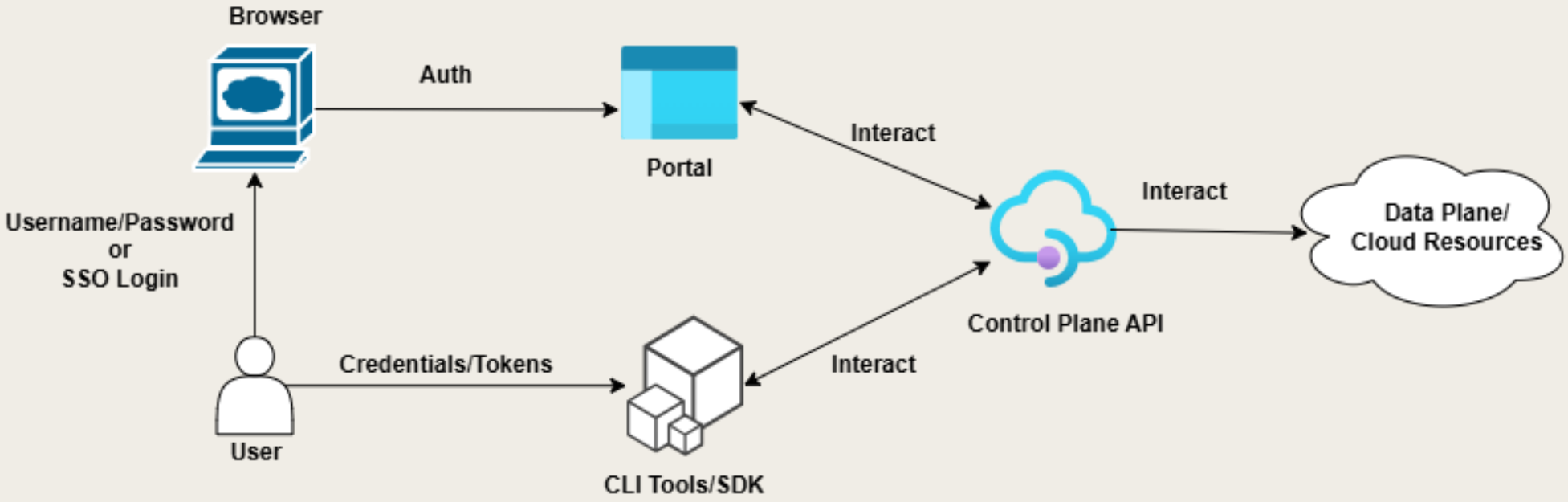
Cloud 101

Cloud 101

Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
Data	Customer responsibility	Customer responsibility	Customer responsibility
Application	Customer responsibility	Customer responsibility	Cloud provider responsibility
Operating system	Customer responsibility	Cloud provider responsibility	Cloud provider responsibility
Virtualization	Cloud provider responsibility	Cloud provider responsibility	Cloud provider responsibility
Servers	Cloud provider responsibility	Cloud provider responsibility	Cloud provider responsibility
Storage	Cloud provider responsibility	Cloud provider responsibility	Cloud provider responsibility
Network	Cloud provider responsibility	Cloud provider responsibility	Cloud provider responsibility
Physical	Cloud provider responsibility	Cloud provider responsibility	Cloud provider responsibility

Cloud 101

- **Control Plane** - Control planes provide the administrative APIs used to create, read/describe, update, delete, and list (CRUDL) resources.
- **Data Plane** – Data plane consists of the systems for consuming those resources, which is basically primary function of the service.



Red Teaming 101

Red Teaming 101

IAM Concepts

Identity and Access Management

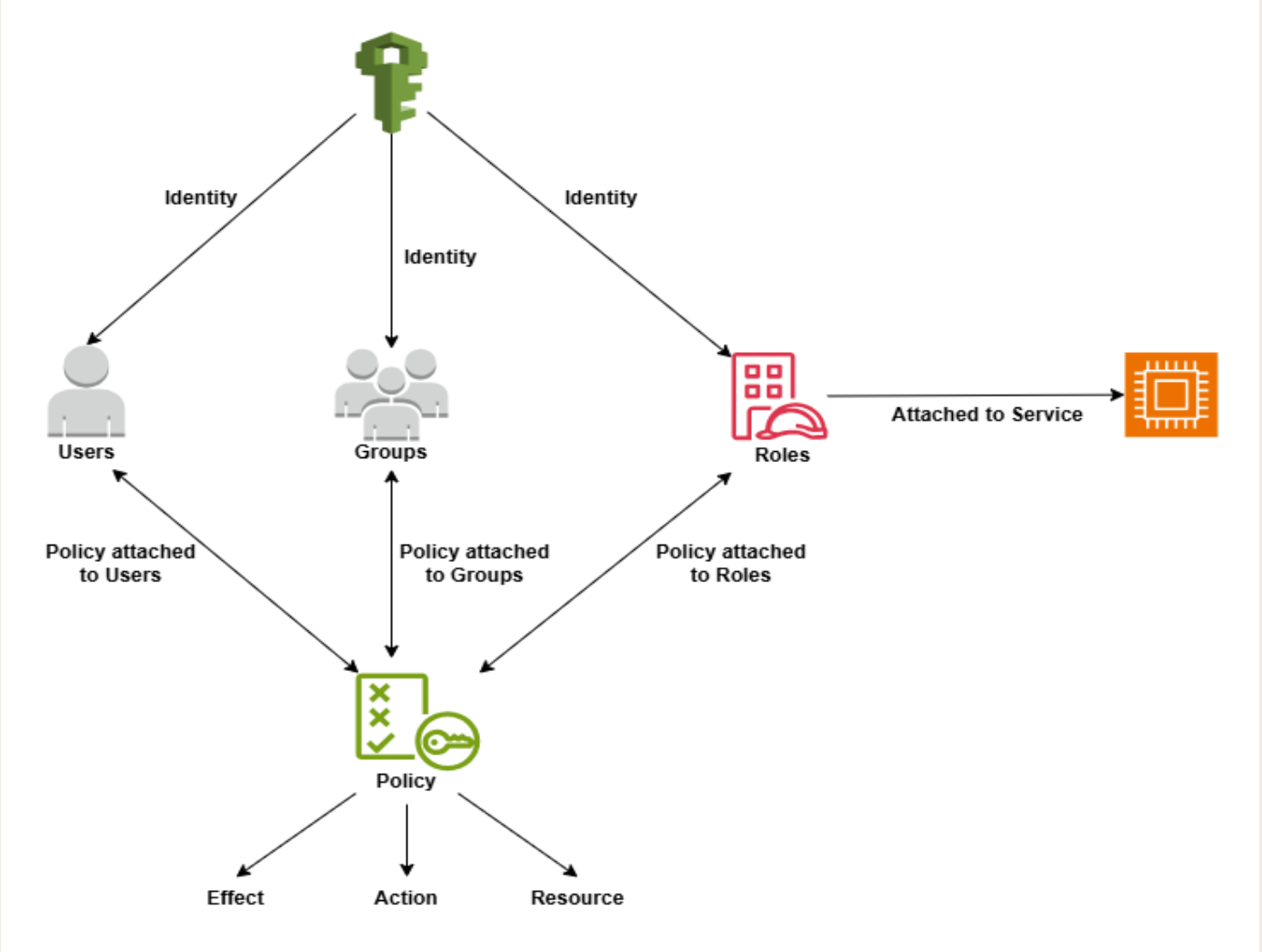
Identity and Access Management (IAM) is the control plane that defines **who** can perform **what** actions on **which resources(where)**, under **what conditions**, and for **how long** using policies evaluated by the providers control plane.

Everything in cloud IAM is *"**Who → What → Where → When → How**"*

Identity and Access Management (IAM)

- Identity/Principal (Who)
- Authenticate
- Authorization (Policy) (What)
- Resource (Where)
- Condition (When)

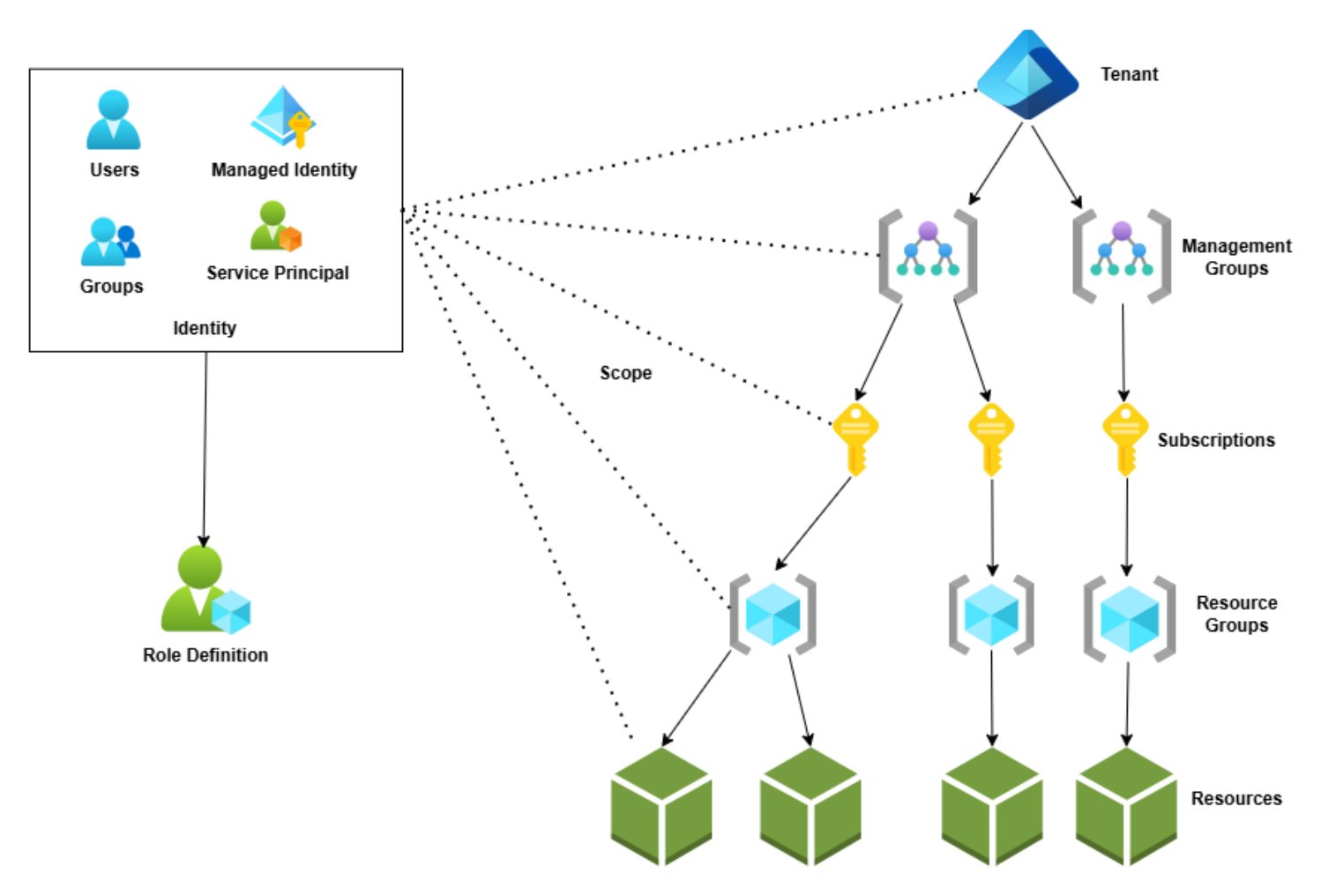
AWS


Identity
Identity
Identity
Users
Groups
Roles
Attached to Service
Policy attached to Users
Policy attached to Groups
Policy attached to Roles
Policy
Effect
Action
Resource

AWS

```
monk@MSI:~$
monk@MSI:~$ aws iam get-policy-version --policy-arn arn:aws:iam::856191759585:policy/
{
    "PolicyVersion": {
        "Document": {
            "Statement": [
                {
                    "Action": "s3:ListBucket",
                    "Effect": "Allow",
                    "Resource": "arn:aws:s3:::cloud-red-lab-internal-752b58"
                },
                {
                    "Action": "s3:GetObject",
                    "Effect": "Allow",
                    "Resource": "arn:aws:s3:::cloud-red-lab-internal-752b58/*"
                }
            ],
            "Version": "2012-10-17"
        },
        "VersionId": "v1",
        "IsDefaultVersion": true,
        "CreateDate": "2025-10-30T15:29:32Z"
    }
}
monk@MSI:~$
```

Azure



Permissions are inherited from top to bottom

Azure

JSON Copy

```
{
  "Name": "Virtual Machine Operator",
  "Id": "88888888-8888-8888-8888-888888888888",
  "IsCustom": true,
  "Description": "Can monitor and restart virtual machines.",
  "Actions": [
    "Microsoft.Storage/*/read",
    "Microsoft.Network/*/read",
    "Microsoft.Compute/*/read",
    "Microsoft.Compute/virtualMachines/start/action",
    "Microsoft.Compute/virtualMachines/restart/action",
    "Microsoft.Authorization/*/read",
    "Microsoft.ResourceHealth/availabilityStatuses/read",
    "Microsoft.Resources/subscriptions/resourceGroups/read",
    "Microsoft.Insights/alertRules/*",
    "Microsoft.Insights/diagnosticSettings/*",
    "Microsoft.Support/*"
  ],
  "NotActions": [],
  "DataActions": [],
  "NotDataActions": [],
  "AssignableScopes": [
    "/subscriptions/{subscriptionId1}",
    "/subscriptions/{subscriptionId2}",
    "/providers/Microsoft.Management/managementGroups/{groupId1}"
  ]
}
```

Common Misconfigurations in Multi-Cloud IAM Setups

Overly Permissive Roles

Roles with excessive permissions increase the risk of unauthorized access and potential data breaches.

Improper Trust Relationships

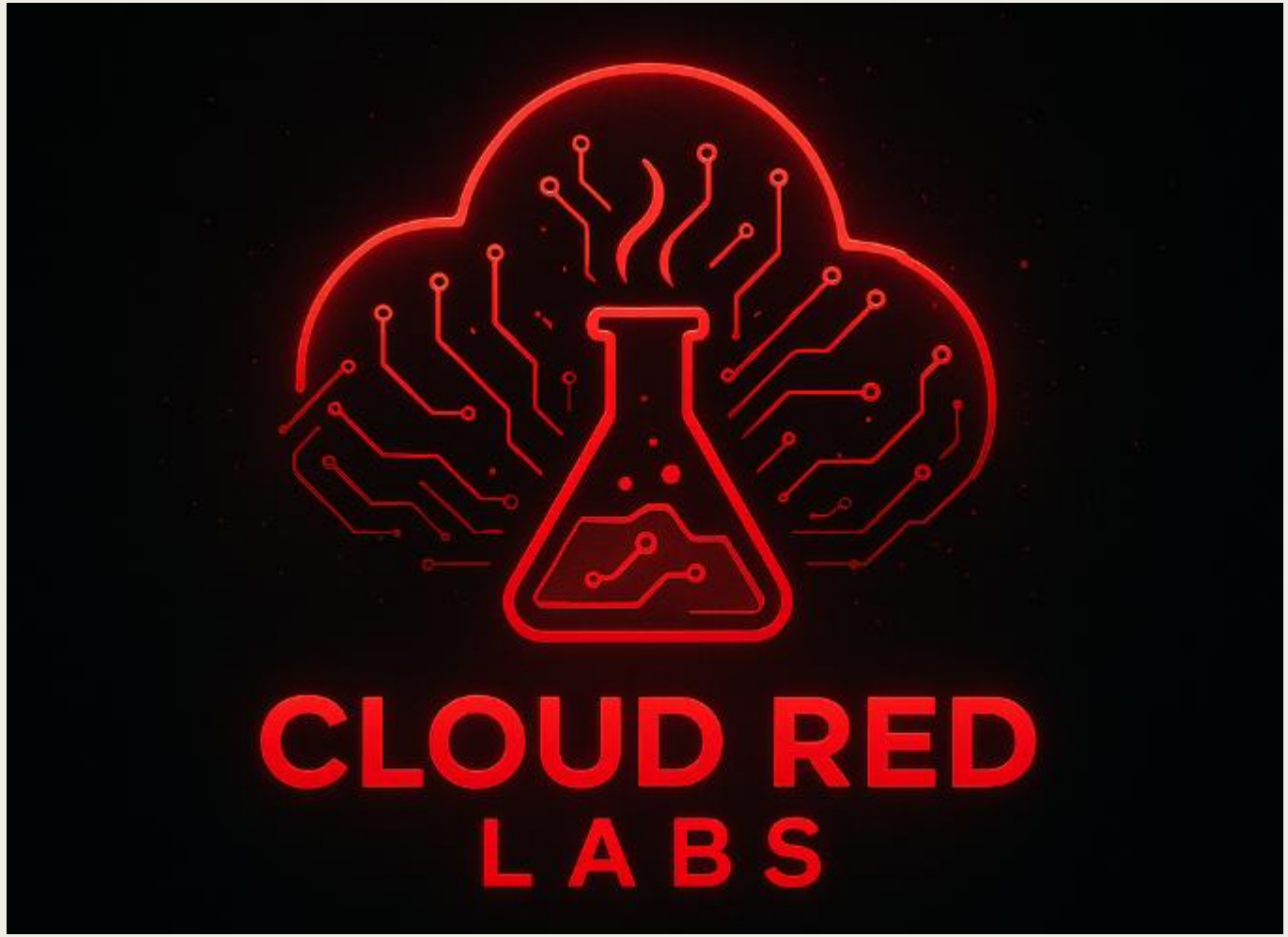
Incorrectly configured trust relationships can allow unintended entities to access sensitive cloud resources.

Inconsistent Policy Management

Discrepancies in policies across clouds create gaps that attackers can exploit for unauthorized access.

Cloud-Red-Labs

Cloud Red Labs



Pre-Requisites

AWS CLI

AZ CLI

Powershell

Defcon Wi-Fi/Backup Hotspot

A Web Browser

Reference Document

Please scan the below to access the application details or navigate to https://shorturl.fm/rn36C

Azure Attack Path

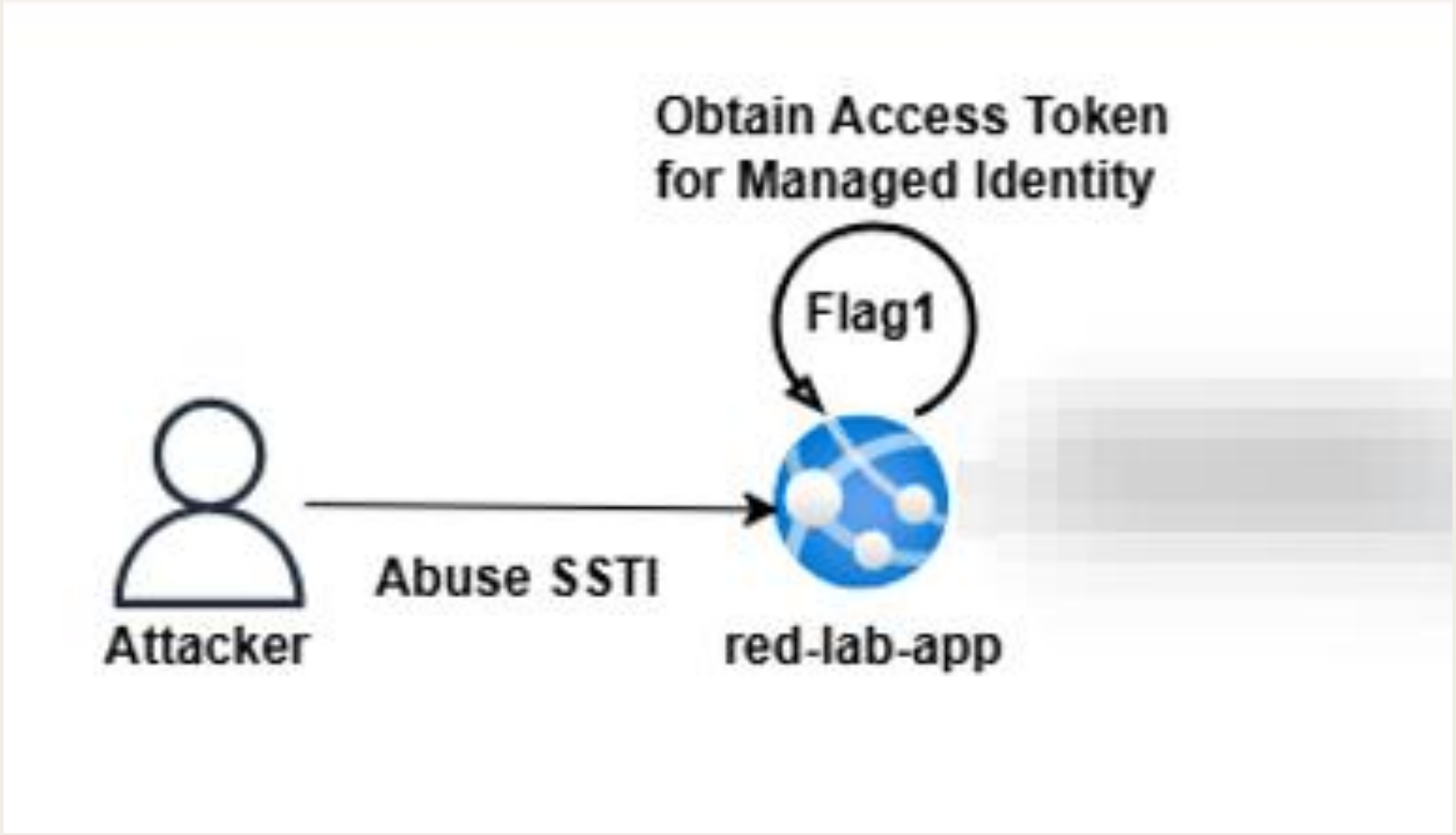
Initial Access

1. Phishing for Users in the Tenant.

2. Exposed secrets.

3. Remote Code Execution by exploitation of Public Facing Infrastructure.

N.B: In this case we will exploit SSTI on an application.


Obtain Access Token
for Managed Identity
Flag1
Abuse SSTI
Attacker
red-lab-app

Internal Recon

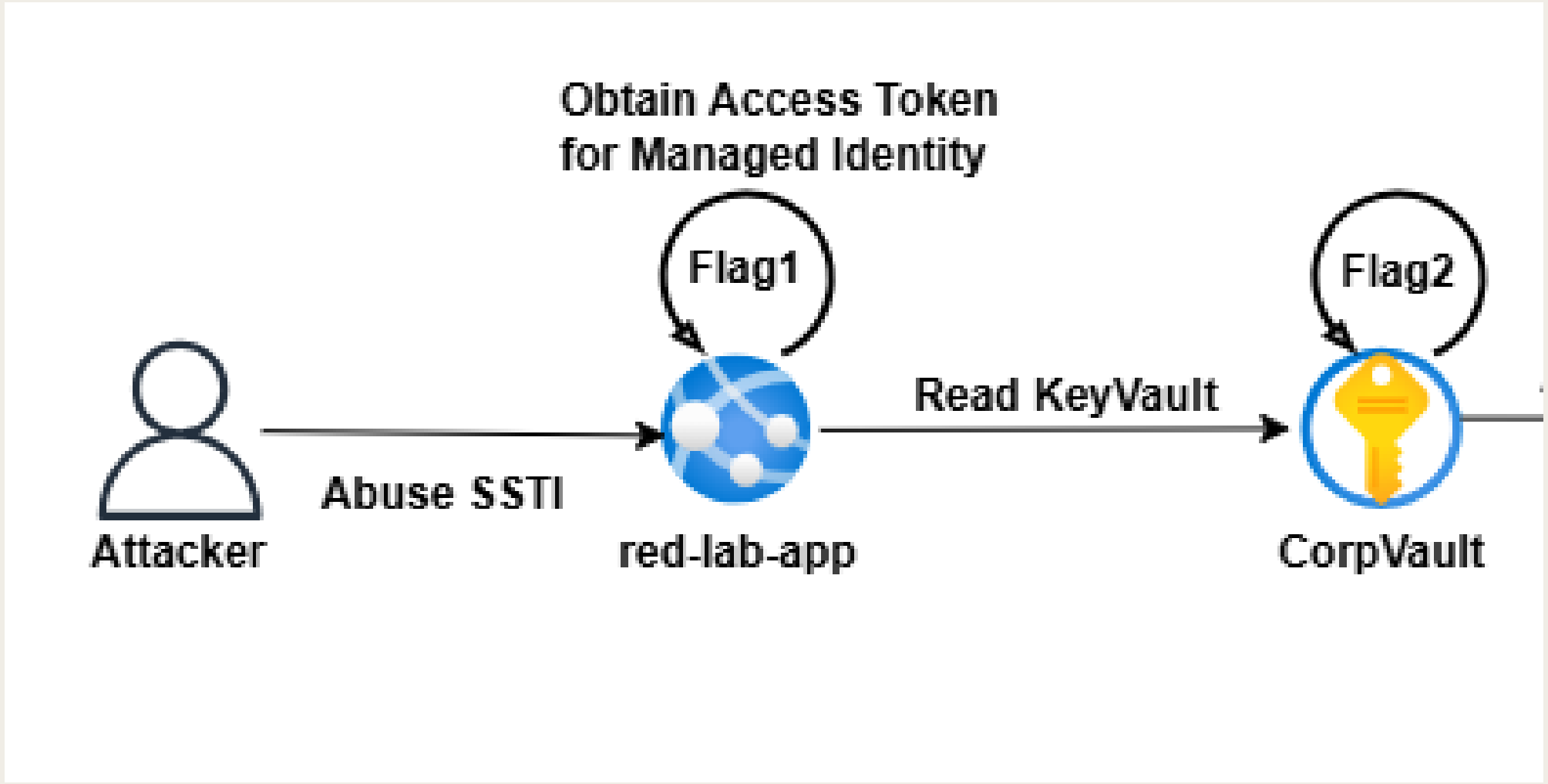
1. Using the Managed Identity token, we can try to enumerate for resources under our given subscription.

2. Look around for common services like Compute, Secret Management and Storage services.

Lateral Movement

1. Using the SSTI, and the correct resource get the Key Vault token.

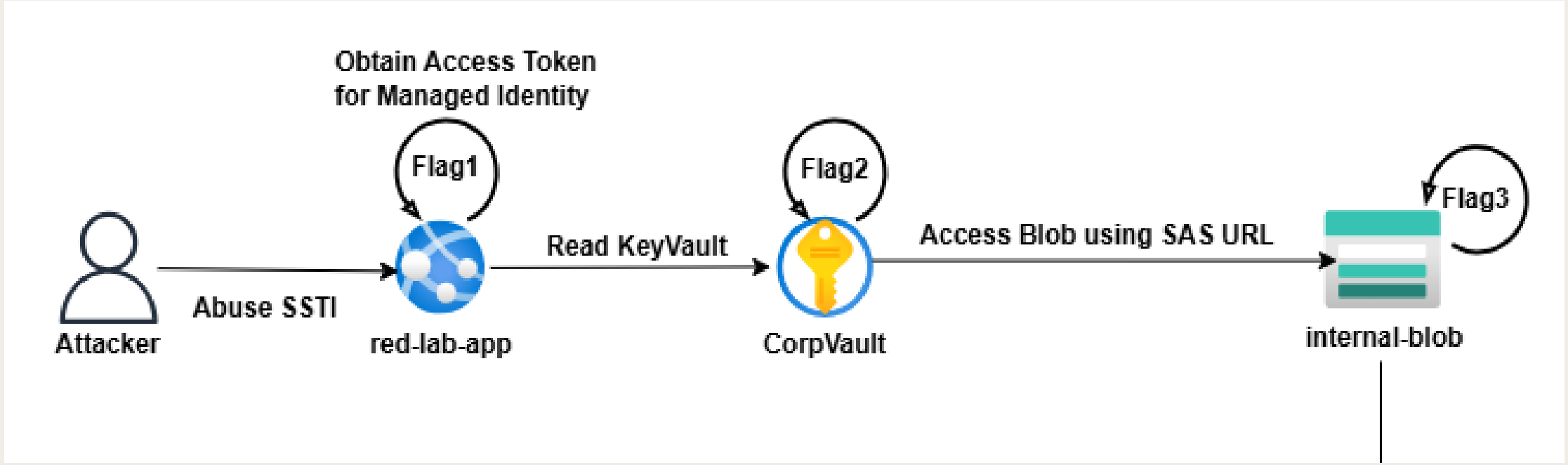
2. Using the Key Vault token try to fetch sensitive data from the Key Vault.

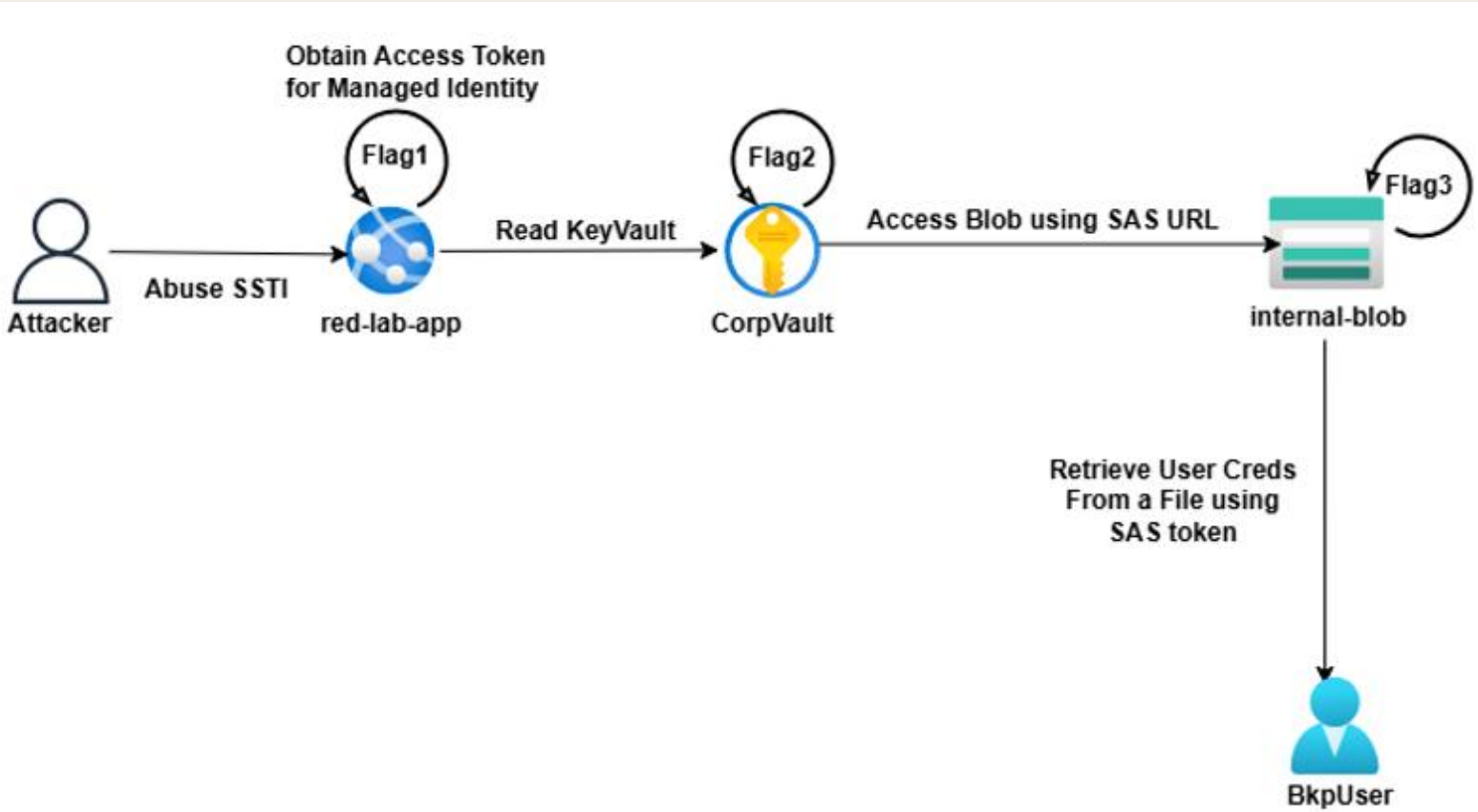

Obtain Access Token
for Managed Identity
Flag1
Flag2
Read KeyVault
Abuse SSTI
Attacker
red-lab-app
CorpVault

Data Exfiltration

1. Using the SAS URL recovered from the Key Vault try to enumerate for other sensitive files.

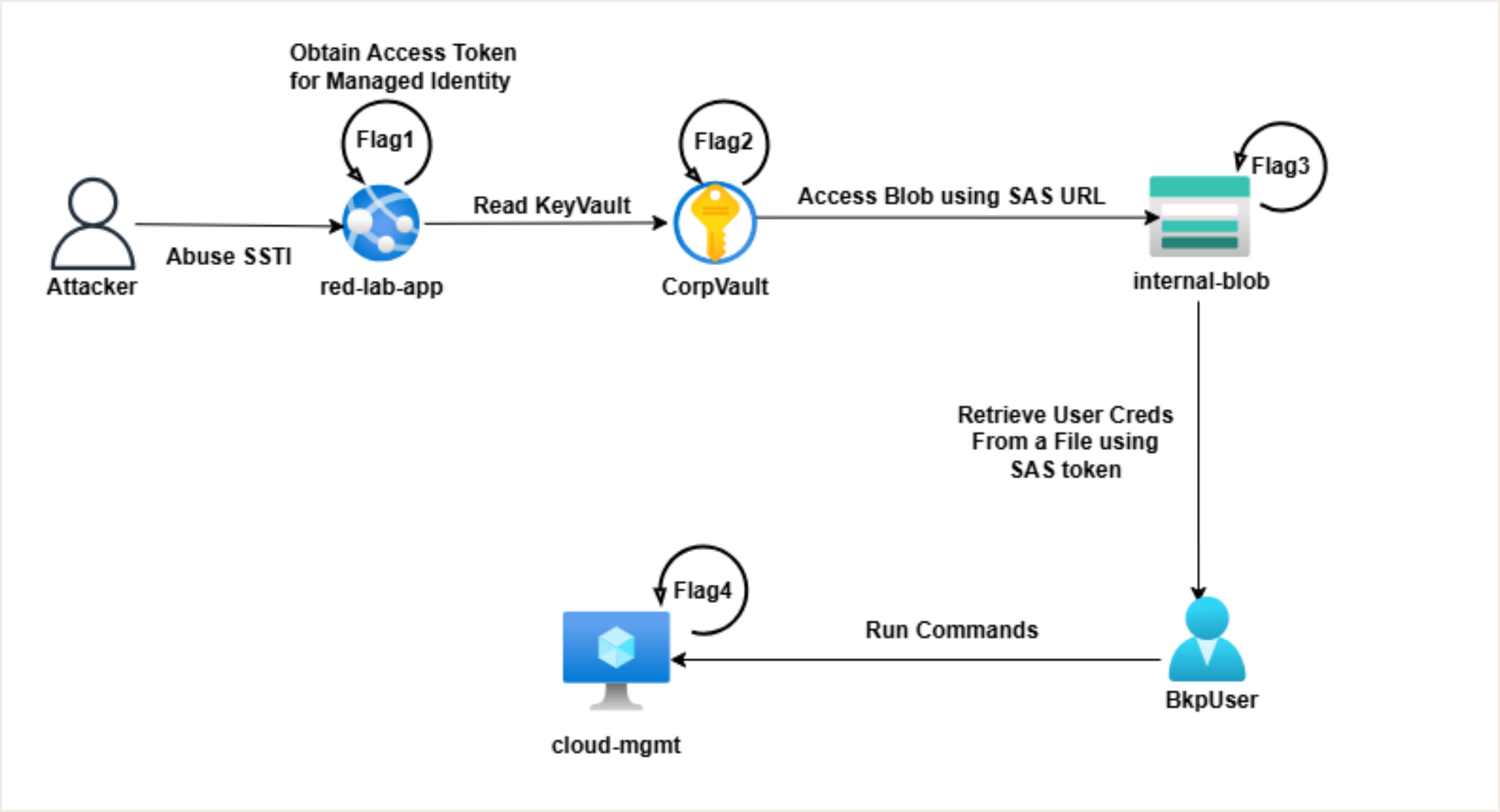
2. Using the files try to gain persistence backdoor to the environment.


Obtain Access Token
for Managed Identity
Flag1
Flag2
Flag3
Read KeyVault
Access Blob using SAS URL
Abuse SSTI
Attacker
red-lab-app
CorpVault
internal-blob


Obtain Access Token
for Managed Identity
Flag1
Flag2
Flag3
Attacker
Abuse SSTI
red-lab-app
Read KeyVault
CorpVault
Access Blob using SAS URL
internal-blob
Retrieve User Creds
From a File using
SAS token
BkpUser

Privilege Escalation

Q. What attack vectors are possible once we compromise the **bkpuser**.


Obtain Access Token
for Managed Identity
Flag1
Flag2
Flag3
Attacker
Abuse SSTI
red-lab-app
Read KeyVault
CorpVault
Access Blob using SAS URL
internal-blob
Retrieve User Creds
From a File using
SAS token
Flag4
Run Commands
BkpUser
cloud-mgmt

AWS Attack Path

Initial Access

1. Phishing for Users in the Cloud.

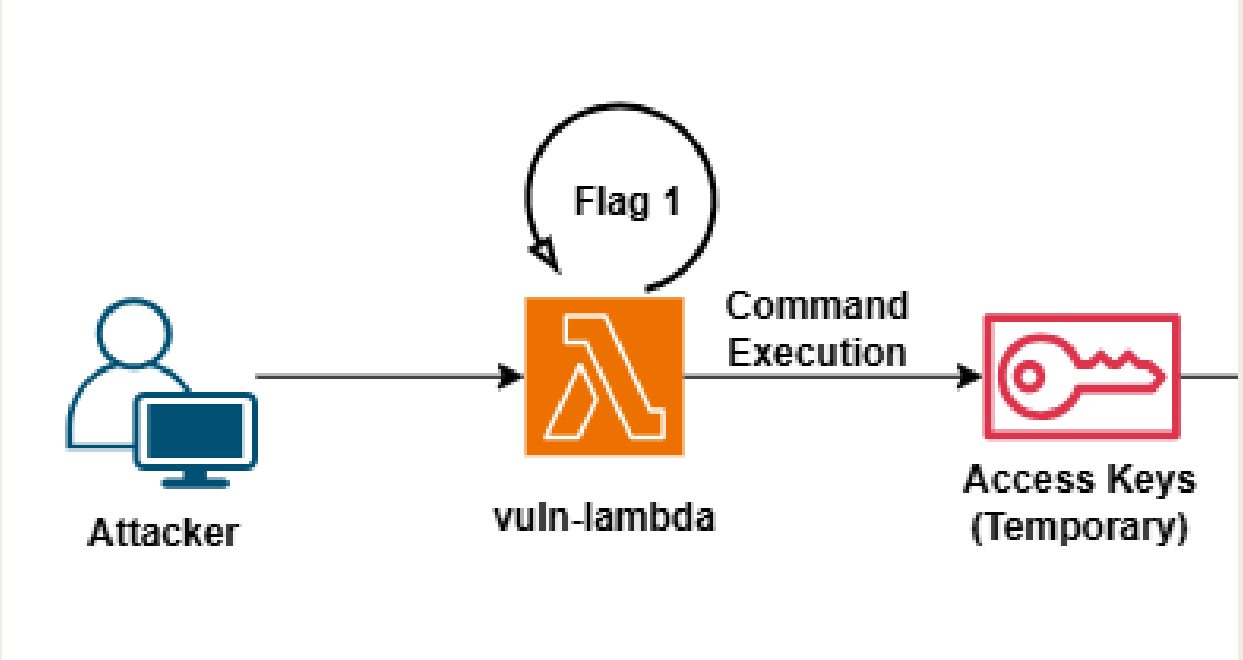
2. Exposed secrets.

3. Remote Code Execution by exploitation of Lambda Function.

N.B: In this case we will exploit command execution on an application.

Initial Access

1. Difference between Short Term and Long-Term Credentials.


Flag 1
Command
Execution
Attacker
vuln-lambda
Access Keys
(Temporary)

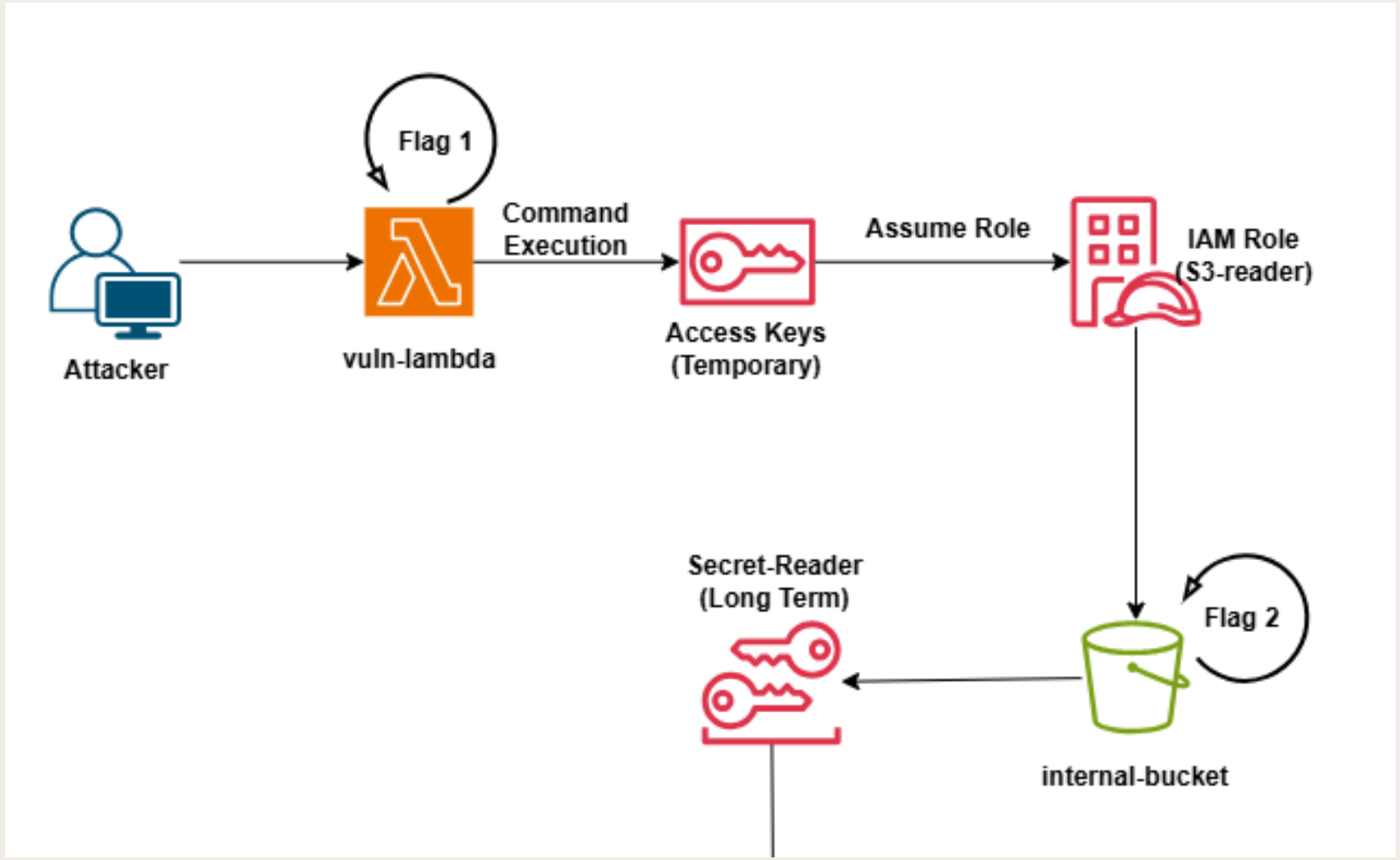
Internal Recon

1. Enumerate the Roles, Permissions and see what services we have access within the environment.

Privilege Escalation and Lateral Movement

1. Assume a role to read secrets from the s3 bucket. (Data Exfiltration)

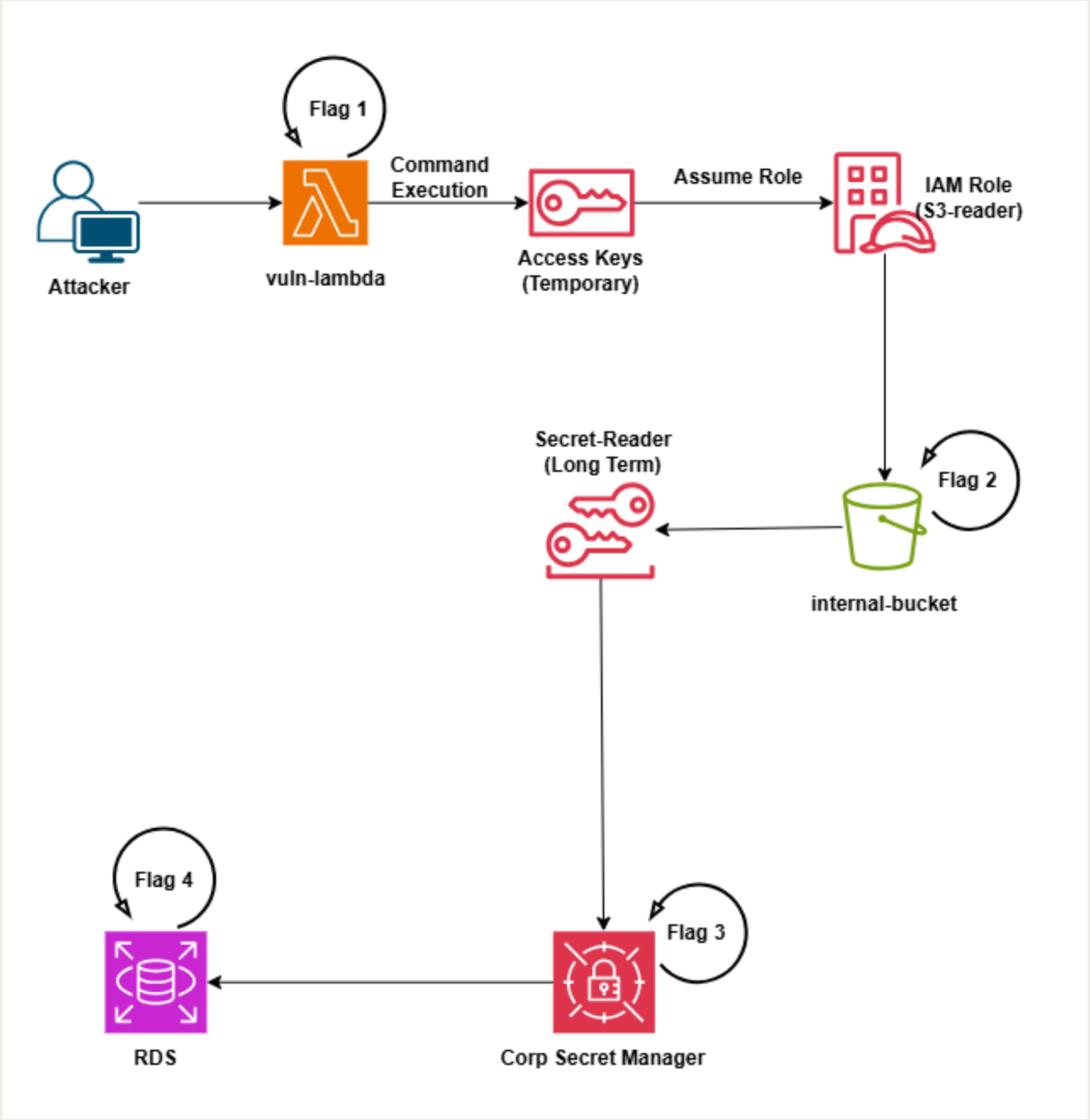
2. Abused the Long-Term Secrets. (Persistence.)


Flag 1
Command
Execution
Assume Role
IAM Role
(S3-reader)
Attacker
vuln-lambda
Access Keys
(Temporary)
Secret-Reader
(Long Term)
Flag 2
internal-bucket

Data Exfiltration

1. Try to extract secrets using the newly found credentials.

Final Task: Use what we have identified so far to find out the Final Flag.


Flag 1
Command Execution
Assume Role
IAM Role (S3-reader)
Attacker
vuln-lambda
Access Keys (Temporary)
Secret-Reader (Long Term)
Flag 2
internal-bucket
Flag 4
Flag 3
RDS
Corp Secret Manager

Detection and Mitigation Strategies

How to Detect and Mitigate

Cloud detection is all about *visibility and correlation*.

Enable logs, feed them into Guard Duty/Defender, and monitor changes to identity, logging, and data access.

Step 1: Collect → Enable logs (CloudTrail / Activity Logs / Sign-in Logs).

Step 2: Analyze → Use Guard Duty or Defender for Cloud to find suspicious patterns.

Step 3: Correlate → Send everything to a SIEM (Security Hub / Sentinel).

Step 4: Respond → Trigger alerts or automated playbooks (disable account, isolate VM).

Q&A