RSAC™ | 2025 Conference

Many Voices.
One Community.

SESSION ID: CTF-T09

Cloud CTF 201: Solving Capture-The-Flag Challenges in AWS, Azure, GCP

Jenko Hwong
Threat Research
WideField Security

Luis Rivas
Network System Engineer
Department of Defense

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

The views and opinions expressed in this presentation are solely those of the speaker and do not represent the views, policies, or positions of the Department of Defense (DoD), the U.S. Army, or any other government agency. This presentation is made in the speaker’s personal capacity and does not constitute an endorsement by the DoD or the U.S. Army.

RSAC | 2025 Conference

MEET THE TEAM

> WHOAMI

Many Voices.
One Community.

Meet the team

Jenko Hwong

linkedin: jenkohwong

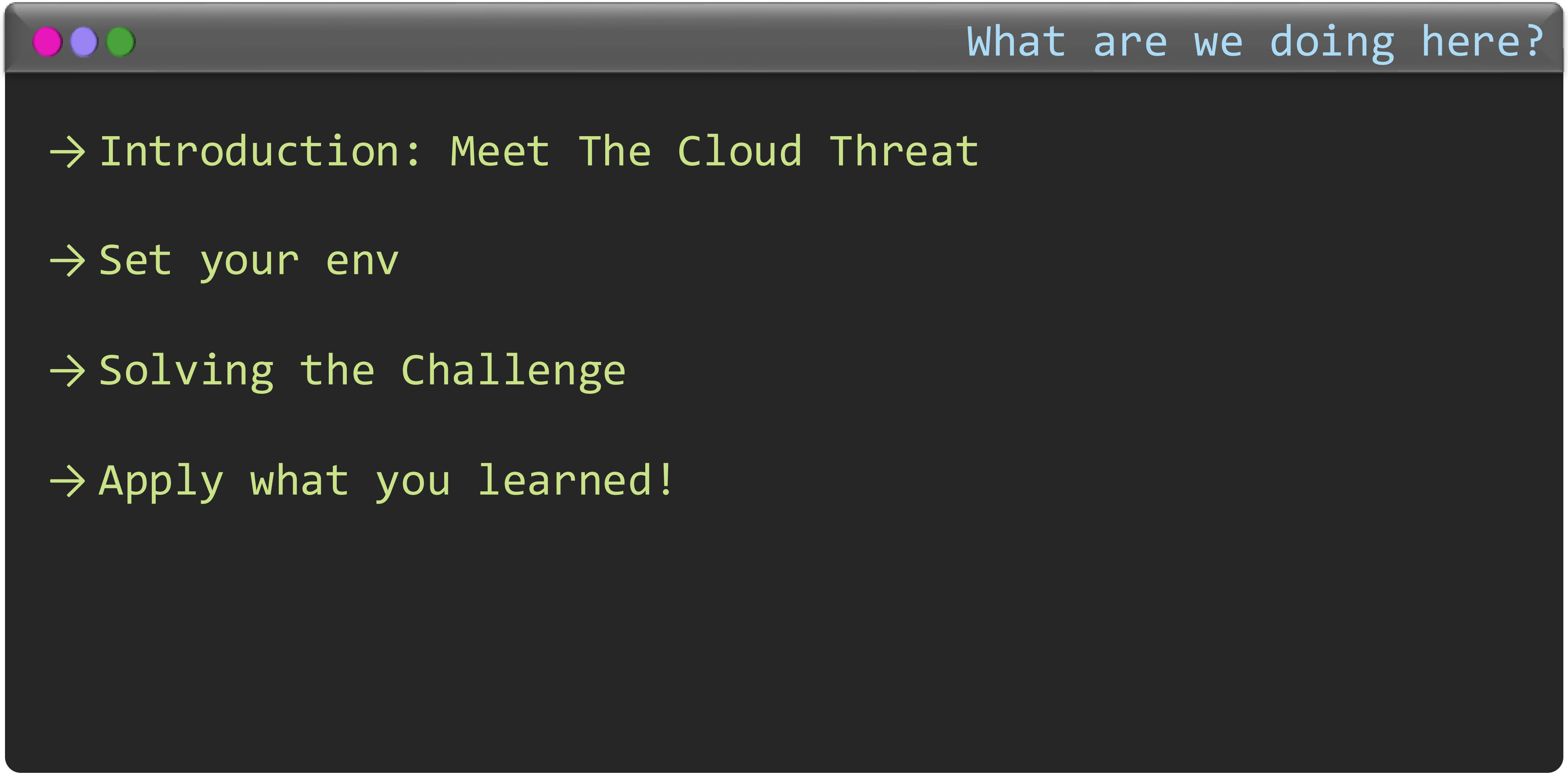
- Cloud threat research, products and engineering
- Vulnerability management, pen-testing, threat intel, AD security
- Contributor Cloud Village CTF

Luis Rivas

GitHub: G0TH3R

- Cybersecurity Researcher and experienced Red Teamer
- Works, learns, and mentors @ Cloud Village
- Over 10 years working with IT, Cybersecurity, and hacks

Agenda



What are we doing here?

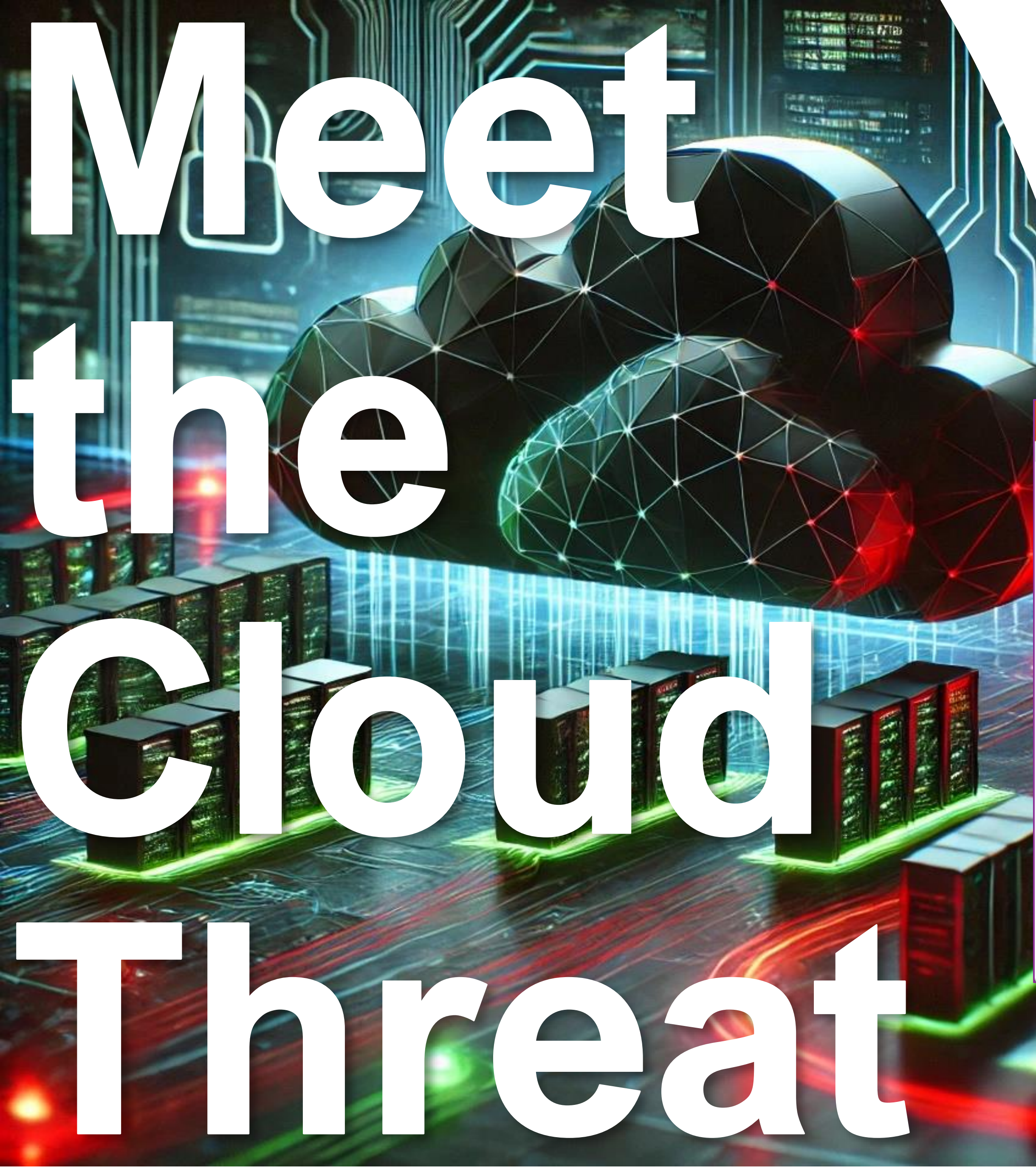
→ Introduction: Meet The Cloud Threat

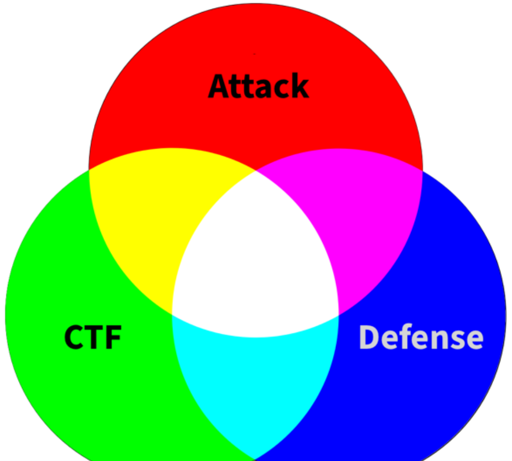
→ Set your env

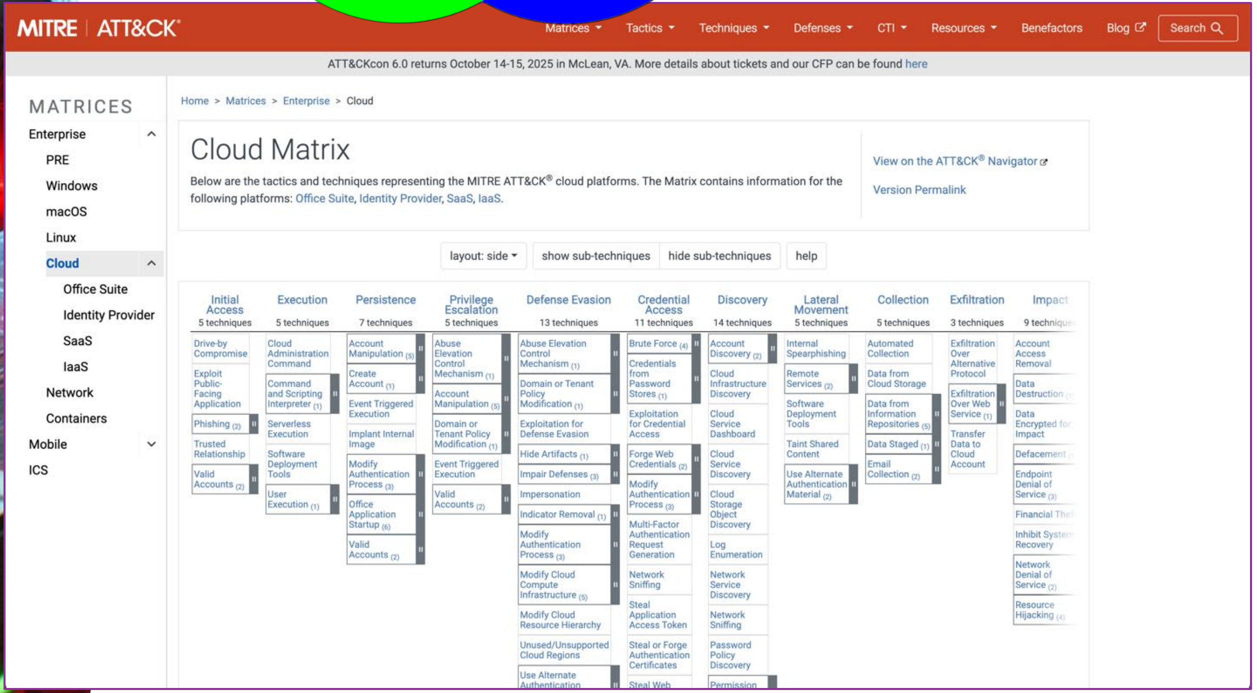
→ Solving the Challenge

→ Apply what you learned!

Meet the Cloud Threat







ATT&CKcon 6.0 returns October 14-15, 2025 in McLean, VA. More details about tickets and our CFP can be found here

MATRICES

- Enterprise
  - PRE
  - Windows
  - macOS
  - Linux
  - Cloud
    - Office Suite
    - Identity Provider
    - SaaS
    - IaaS
  - Network
  - Containers
- Mobile
- ICS

Home > Matrices > Enterprise > Cloud

Cloud Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® cloud platforms. The Matrix contains information for the following platforms: Office Suite, Identity Provider, SaaS, IaaS.

View on the ATT&CK® Navigator

Version Permalink

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Impact
5 techniques	5 techniques	7 techniques	5 techniques	13 techniques	11 techniques	14 techniques	5 techniques	5 techniques	3 techniques	9 techniqu
Drive-by Compromise	Cloud Administration Command	Account Manipulation (5)	Abuse Elevation Control Mechanism (1)	Abuse Elevation Control Mechanism (1)	Brute Force (4)	Account Discovery (2)	Internal Spearphishing	Automated Collection	Exfiltration Over Alternative Protocol	Account Access Removal
Exploit Public-Facing Application	Command and Scripting Interpreter (1)	Create Account (1)	Account Manipulation (5)	Domain or Tenant Policy Modification (1)	Credentials from Password Stores (1)	Cloud Infrastructure Discovery	Remote Services (2)	Data from Cloud Storage	Exfiltration Over Web Service (1)	Data Destruction (1)
Phishing (2)	Serverless Execution	Event Triggered Execution	Domain or Tenant Policy Modification (1)	Exploitation for Defense Evasion	Exploitation for Credential Access	Cloud Service Dashboard	Software Deployment Tools	Data from Information Repositories (5)	Transfer Data to Cloud Account	Data Encrypted for Impact
Trusted Relationship	Software Deployment Tools	Implant Internal Image	Event Triggered Execution	Hide Artifacts (1)	Forge Web Credentials (2)	Cloud Service Discovery	Taint Shared Content	Data Staged (1)		Defacement
Valid Accounts (2)	User Execution (1)	Modify Authentication Process (3)	Valid Accounts (2)	Impair Defenses (3)	Modify Authentication Process (3)	Cloud Storage Object Discovery	Use Alternate Authentication Material (2)	Email Collection (2)		Endpoint Denial of Service (3)
		Office Application Startup (6)		Impersonation	Multi-Factor Authentication Request Generation	Log Enumeration				Financial Thef
		Valid Accounts (2)		Indicator Removal (1)	Network Sniffing	Network Service Discovery				Inhibit System Recovery
				Modify Authentication Process (3)	Steal Application Access Token	Network Sniffing				Network Denial of Service (2)
				Modify Cloud Compute Infrastructure (5)	Steal or Forge Authentication Certificates	Password Policy Discovery				Resource Hijacking (4)
				Modify Cloud Resource Hierarchy	Steal Web	Permission				
				Unused/Unsupported Cloud Regions						
				Use Alternate Authentication						

Using a common framework

RSAC 2025 Conference

AWS

Many Voices.
One Community.

Threat Actor:
APT-909 "Nebula Specters"

Cloud-native adversary targeting DevOps pipelines, cloud IAM misconfigurations, and ephemeral credentials.

Tactics & Techniques:

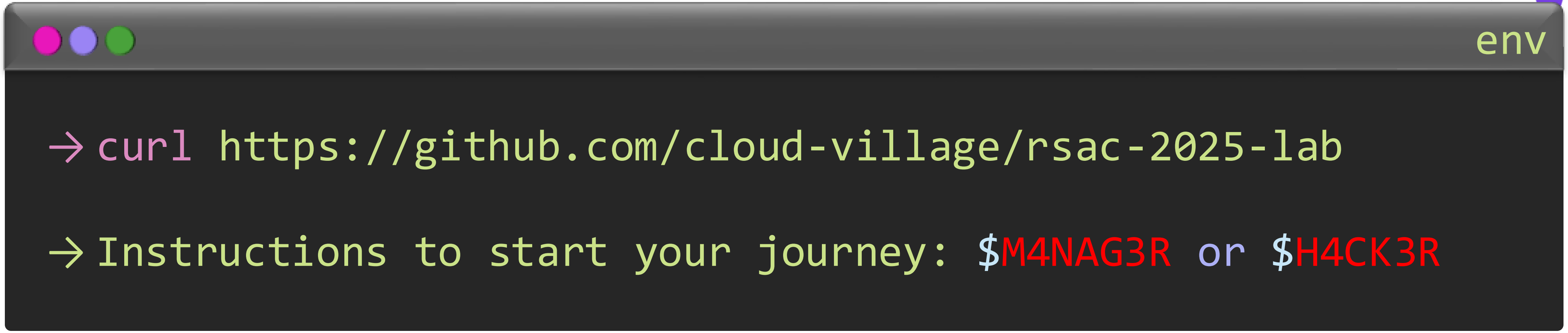
- **T1087.004** - Cloud Account Discovery
- **T1552.005** - Unsecured Credentials in Instance Metadata Service
- **T1078.004** - Cloud Accounts with Misconfigured Role Assumption

Objective:

(C) Persistence & Data Exfiltration from AWS

CLASSIFIED

Set your environment



```
→ curl https://github.com/cloud-village/rsac-2025-lab

→ Instructions to start your journey: $M4NAG3R or $H4CK3R
```

CHOOSE YOUR ADVENTURE

Solving the Challenge: AWS

→

→

→

→ AWS Challenge << EOF > solution.md

BLOG // TECH // SEP 13, 2022

Introducing: CloudFox

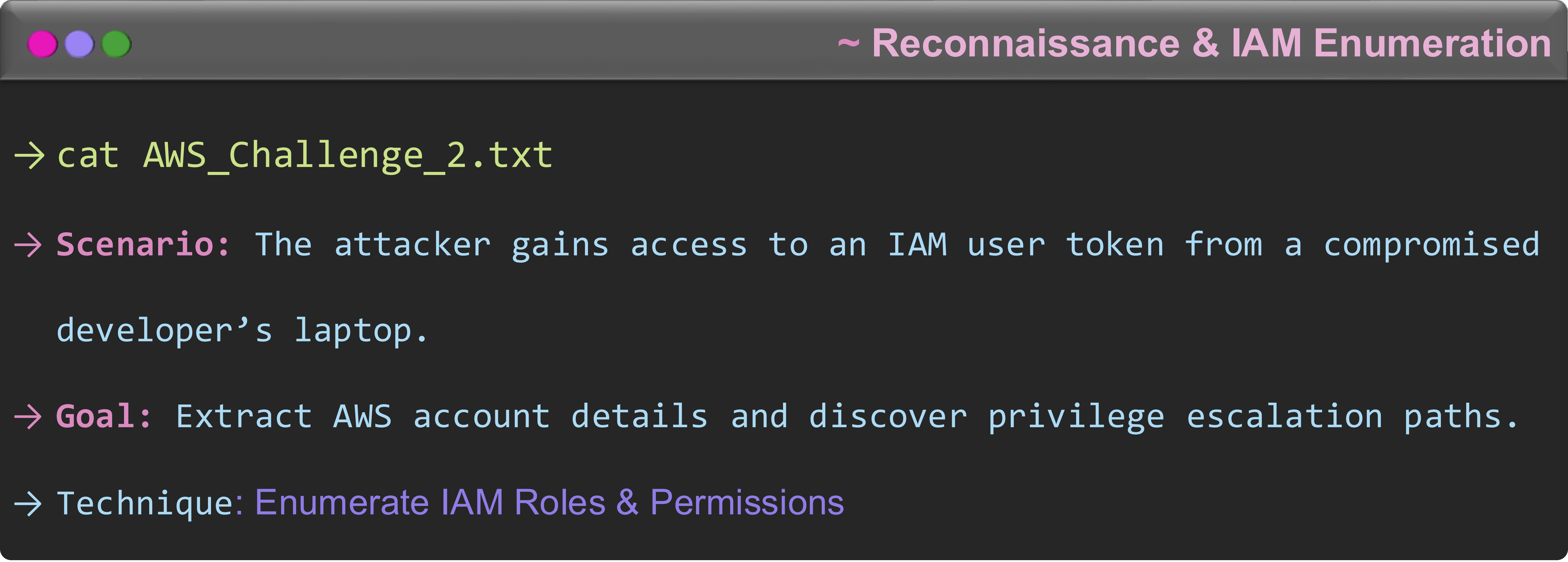
By: Seth Art, Alumnus Principal Security Consultant & Carlos Vendramini, Bishop Fox Alumnus

Choose your Tools!

~ Exploiting EC2 Instance Metadata for Temporary Credentials

```
→ cat AWS_Challenge_1.txt

→ Scenario: A misconfigure EC2 instance allows APT 909 metadata service

  (IMDSv1) access.

→ Goal: Extract Temporary AWS Credentials.

→ Technique: Abuse EC2 Metadata API
```

```
Defensive Measures:
   Enforce IMDSv2, restrict IAM roles, monitor VPC Flow Logs
```



~ Reconnaissance & IAM Enumeration

```
→ cat AWS_Challenge_2.txt

→ Scenario: The attacker gains access to an IAM user token from a compromised
  developer’s laptop.

→ Goal: Extract AWS account details and discover privilege escalation paths.

→ Technique: Enumerate IAM Roles & Permissions
```

Defensive Measures:
CloudTrail logging, IAM least privilege, GuardDuty alerts.

~ Privilege Escalation and Data Exfiltration

```
→ cat AWS_Challenge_3.txt

→ Scenario: The attacker finds an overprivileged IAM role that allows

  sts:AssumeRole and access to S3 bucket.

→ Goal: Move laterally by assuming a more privileged role and exfil data.

→ Technique: IAM Role Hijacking and S3 Accessible S3 Buckets
```

Defensive Measures:
Restrict sts:AssumeRole, enable CloudTrail and bucket monitoring

GCP

Many Voices.
One Community.

Threat Actor:
UNC-225 "Evil Corp"

Cloud-native adversary targeting DevOps pipelines, cloud IAM misconfigurations, and ephemeral credentials.

Tactics & Techniques:

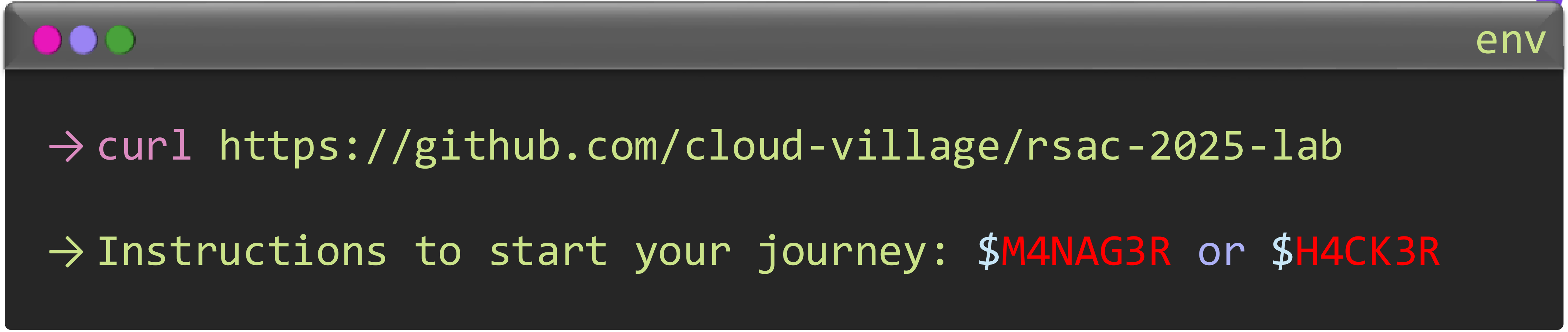
T1486.000 – Data Encrypted for Impact
T1552.005 - Unsecured Credentials in Instance Metadata Service
T1078.004 - Cloud Accounts with Misconfigured Role Assumption

Objective:

(C) Persistence & Data Exfiltration from GCP

CLASSIFIED

Set your environment



```
→ curl https://github.com/cloud-village/rsac-2025-lab

→ Instructions to start your journey: $M4NAG3R or $H4CK3R
```

CHOOSE YOUR ADVENTURE

Solving the Challenge

```
→

→

→

→  GCP Challenge << EOF > solution.md
```

~ Supply Chain Attack via Cloud Build Poisoning

```
→ cat GCP_Challenge_1.txt

→ Scenario: A DevOps pipeline in Cloud Build is injected with malicious

  artifacts.

→ Goal: Inject a backdoored artifact into Cloud Build to gain access.

→ Technique: Cloud Build Privilege Escalation & Artifact Poisoning
```

```
Defensive Measures:
   Monitor for unauthorized Cloud Build Modifications
   Limit Cloud Build to only necessary permissions
   Enforce Binary Authorization to prevent unsigned deployments
```

~ Escaping a GKE Container to Compromise the Host

```
→ cat GCP_Challenge_2.txt

→ Scenario: A cluster allows attackers to escape and gain host-level.

→ Goal: Exploit GKE misconfigurations to escape a container and execute

  commands on the underlying host.

→ Technique: Kubernetes privilege Escalation + Escape to Host
```

Defensive Measures:
Pod Security Policies: Prevent containers from running as root.
Restrict Kubernetes RBAC: Ensure least privilege
Cloud Logging: Monitor unusual Kubernetes API calls

Azure

Threat Actor:
Storm-2025 "Rosa Klebb"

Cloud-native adversary targeting OAuth tokens, service principals, and native services.

Tactics & Techniques:

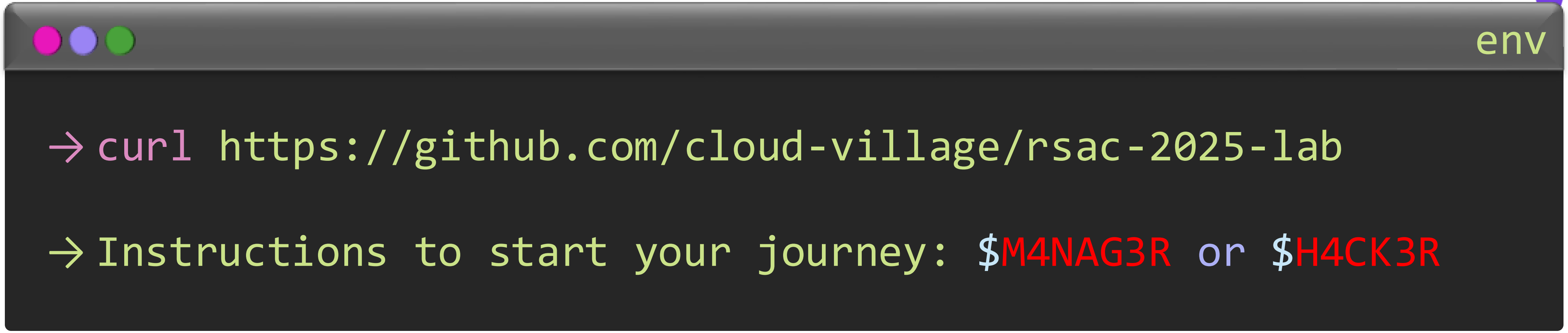
- **T1550.001** – Application Access Token
- **T1556.009** – Conditional Access Policies
- **T1078.004** - Cloud Accounts

Objective:

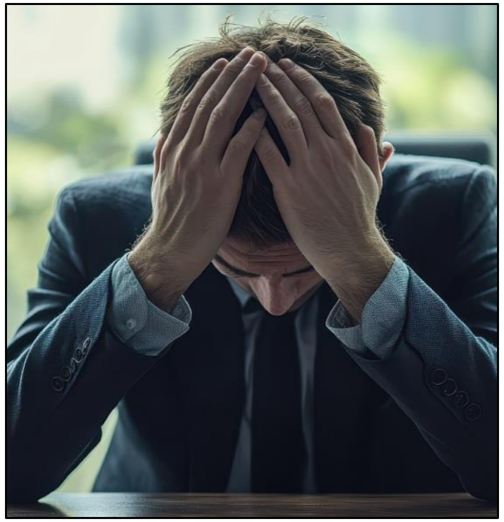
(C) Defense Evasion & Persistence

CLASSIFIED

Set your environment



```
→ curl https://github.com/cloud-village/rsac-2025-lab

→ Instructions to start your journey: $M4NAG3R or $H4CK3R
```



CHOOSE YOUR ADVENTURE

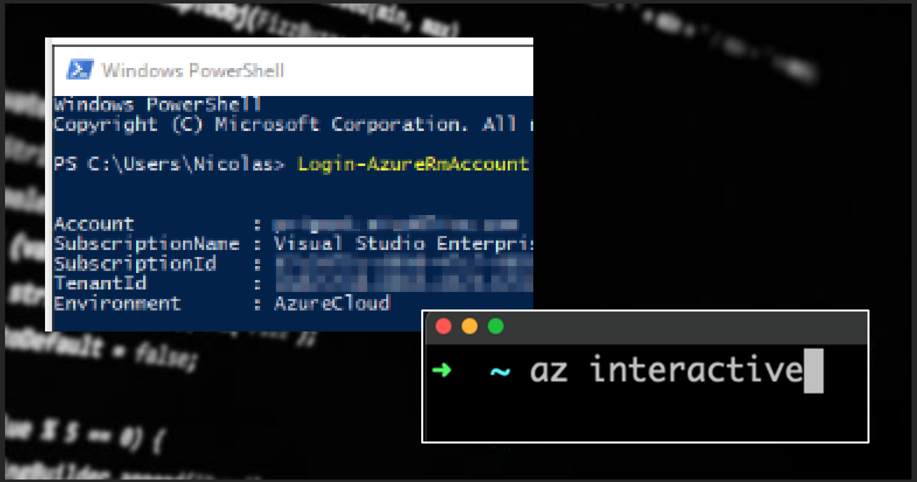
Solving the Challenge: AWS

→

→

→

→ Azure Challenge << EOF > solution.md



```
Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All r
PS C:\Users\Nicolas> Login-AzureRmAccount

Account          : [redacted]
SubscriptionName : Visual Studio Enterpri
SubscriptionId   : [redacted]
TenantId         :
Environment      : AzureCloud
```

```
→ ~ az interactive
```

Choose your Tools!

~ Privilege Escalation and Data Exfiltration

```
→ cat Azure_Challenge_1.txt

→ Scenario: Weak authentication policies lead to session hijacking and access.

→ Goal: Enumerate users, password-spray, discover targets, spear-phish.

→ Technique: Use enumeration and password spray, MSGraph calls, and device code phish.
```

Defensive Measures:
Entra ID hardening, user types, MFA, and Conditional Access.

~ Privilege Escalation and Data Exfiltration

→ cat Azure_Challenge_2.txt

→ **Scenario:** Service principals allow privilege escalation.

→ **Goal:** Exploit App Administrator access to gain control of an SP.

→ Technique: az ad sp, aadinternals

Defensive Measures:
Restricted roles, strong SP auth, Azure log monitoring.

~ Privilege Escalation and Data Exfiltration

→ cat Azure_Challenge_3.txt

→ **Scenario:** Post access, you want to install backdoors for persistence.

→ **Goal:** Use temporary delete status, Cloud Shells, service principals, and Serverless functions for persistence.

→ Technique: custom

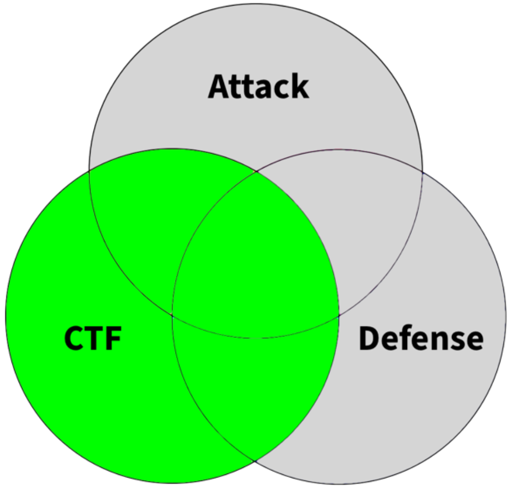
Defensive Measures:
Restricted roles, strong SP auth, Azure log monitoring.

Learnings

Many Voices.
One Community.

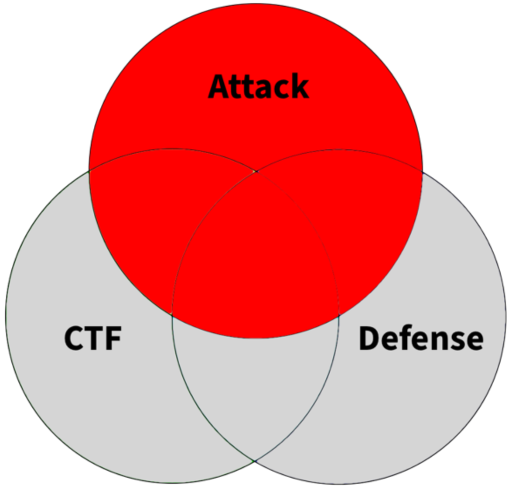
“Apply” CTF in Life

- CTF is a playground
  - Sharpen your skills in CTFs
  - Seek out and share knowledge
  - Have fun and learn
- The office is the battleground
  - Map to real red-team techniques
  - Anticipate defensive measures as you solve challenges
  - Teamwork



“Apply” the Adversarial Perspective

- The ignored attack chain
  - Enumeration and discovery are ignored
  - Persistence is not just a good red-team trait
  - Cloud log evasion and confusion
- Techniques
  - Session tokens are a gift that keeps giving
  - Confused identities are an opportunity
- “Know thy adversary”
  - IPs, domains, URLs – exploit the trust and hide in the noise
  - Posture/config, MFA, conditional access, primary credentials



“Apply” Defense in Depth

- Cybersecurity is everyone’s realm

  Protect it.

- Learn more about attacks – Understand how to defend

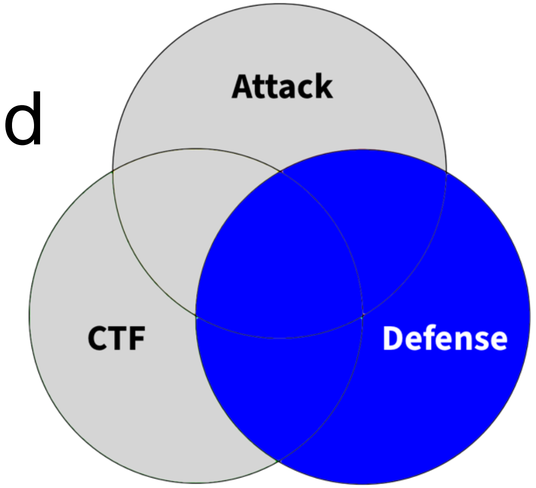
  Zero Trust will not defend itself.

- Analyze broadly

  Implement incrementally.

- Some defense is better than NO Defense

  You are ready.



Resources

Many Voices.
One Community.

Code and Explanations

- https://github.com/cloud-village/rsac-2025-lab

```
README.md
Technical_Notes.pdf
Solutions.pdf
AWS/
Azure/
GCP/
Tools/
```

RSAC™ 2025 Conference

Many Voices.
One Community.

RSAC 2025 Conference

Azure Challenge Walkthrough

Many Voices.
One Community.

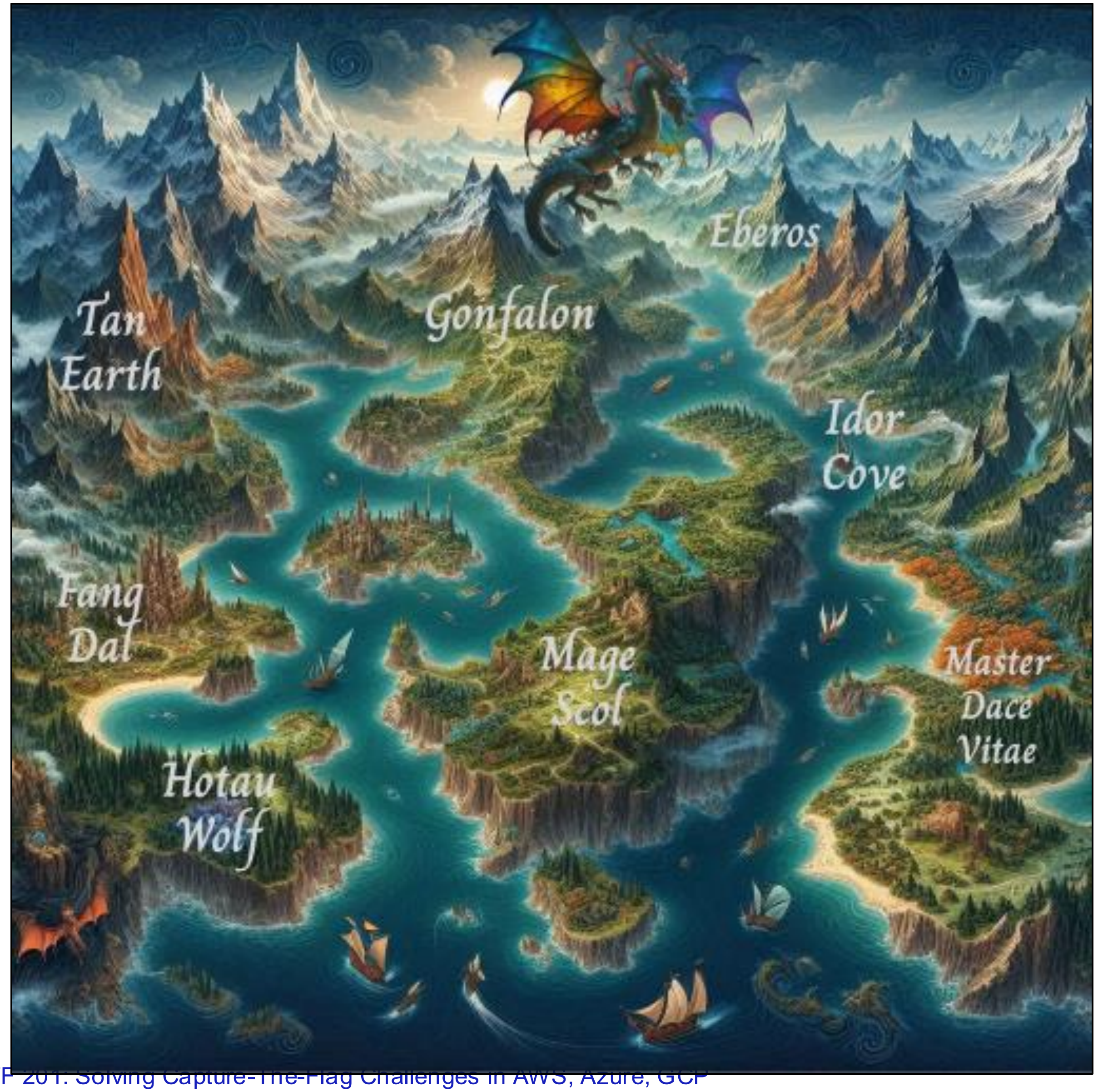
General

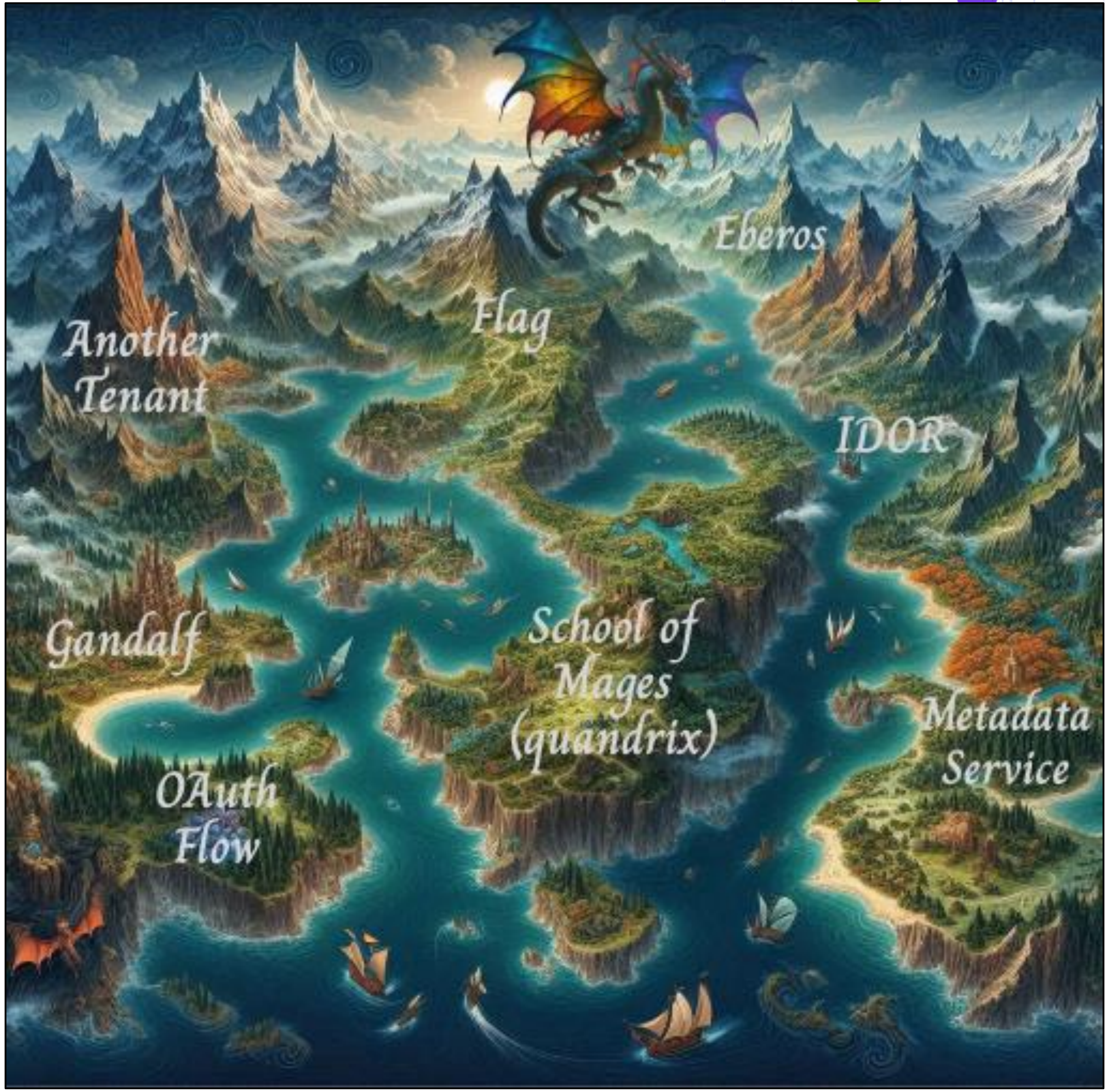
- Hard to Insane Azure Challenge
- Azure TTP focus
- Heavy game theme/puzzles (mixed)
- Tried to use recent real-world TTP
  - User **discovery**
  - OAuth device code **phish**
  - Microsoft SSO (Azure - Apps)
  - Lateral movement / stealth (tenant #2, **deleteItems**)

Starting point

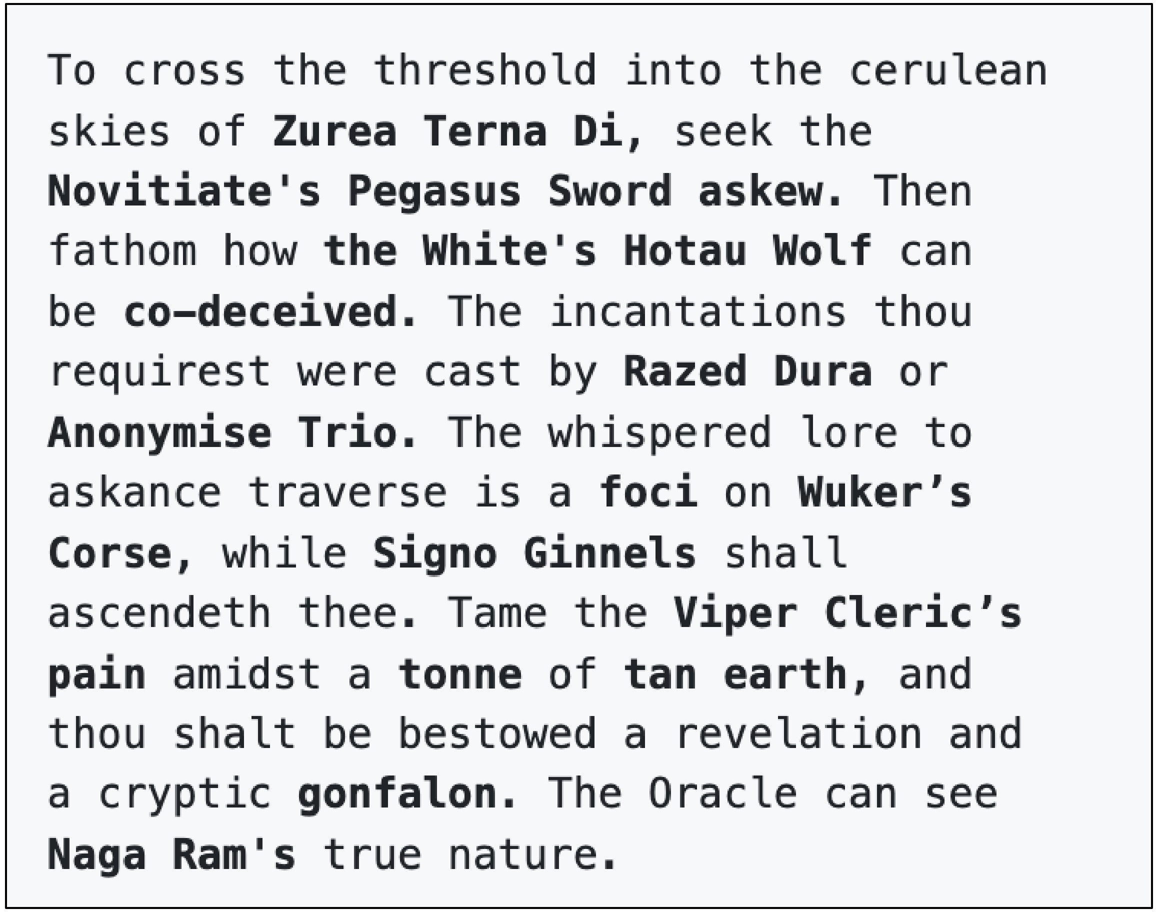
- http://erebos0.cloudy-daze.com:8080
- HTTP Auth user: idq
- HTTP Auth pwd: XXXXXXX

The Map

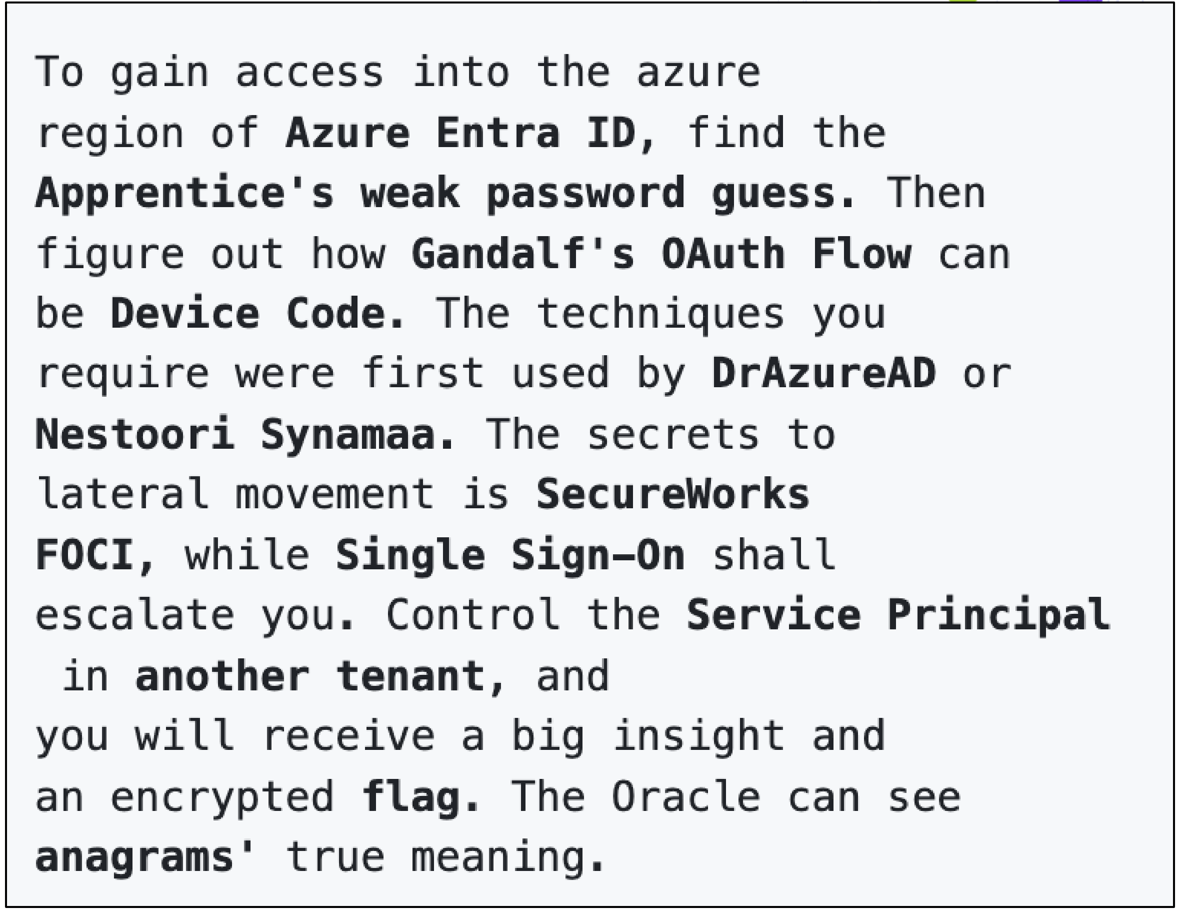

Eberos
Tan Earth
Gonfalon
Idor Cove
Fang Dal
Mage Scol
Master Dace Vitae
Hotau Wolf


Eberos
Another Tenant
Flag
IDOR
Gandalf
School of Mages (quandrix)
Metadata Service
OAuth Flow

The Scroll

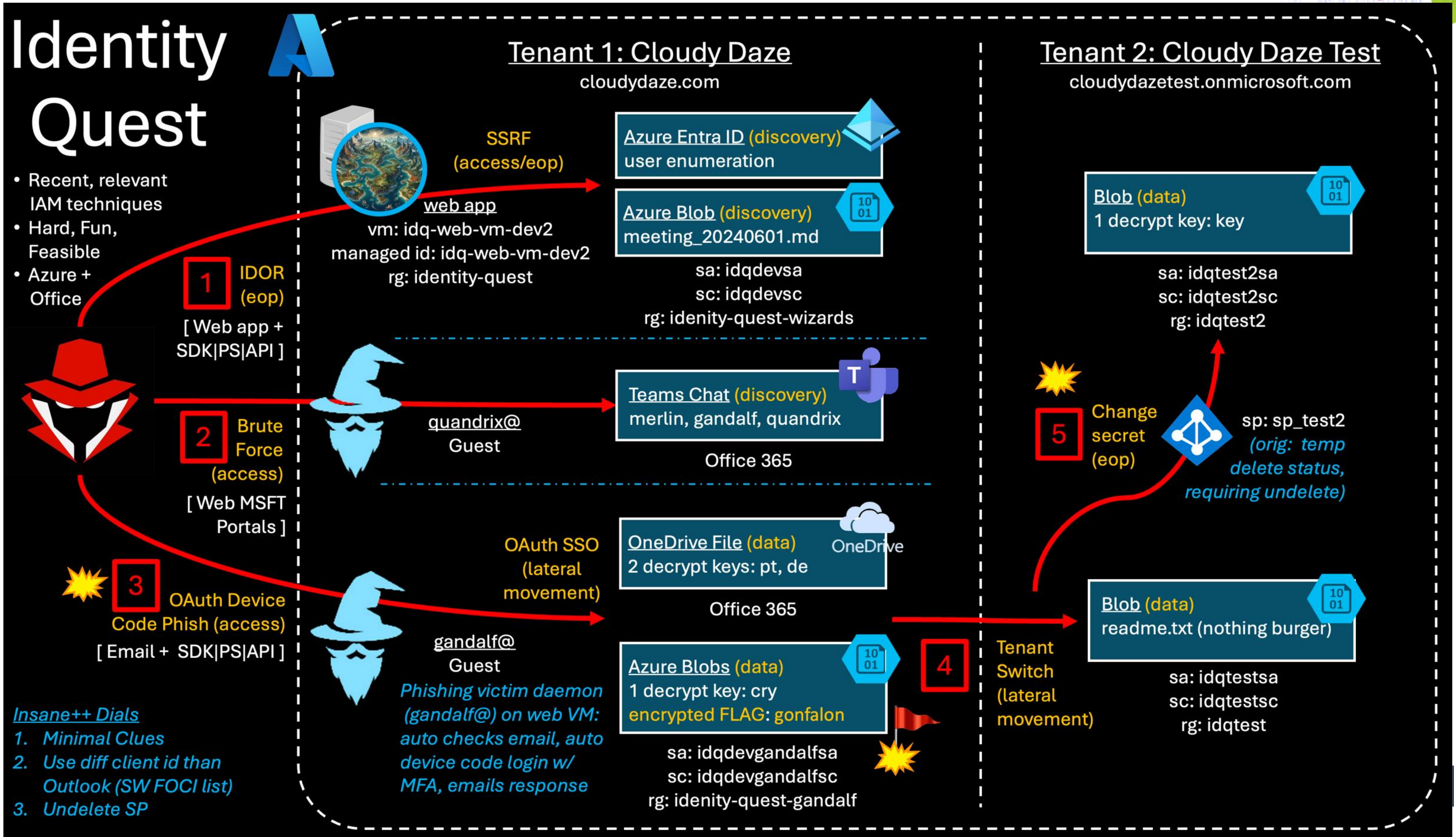


To cross the threshold into the cerulean skies of **Zurea Terna Di**, seek the **Novitiate's Pegasus Sword askew.** Then fathom how **the White's Hotau Wolf** can be **co-deceived.** The incantations thou requirest were cast by **Razed Dura** or **Anonymise Trio.** The whispered lore to askance traverse is a **foci** on **Wuker's Corse**, while **Signo Ginnels** shall ascendeth thee. Tame the **Viper Cleric's pain** amidst a **tonne** of **tan earth**, and thou shalt be bestowed a revelation and a cryptic **gonfalon.** The Oracle can see **Naga Ram's** true nature.



To gain access into the azure region of **Azure Entra ID**, find the **Apprentice's weak password guess.** Then figure out how **Gandalf's OAuth Flow** can be **Device Code.** The techniques you require were first used by **DrAzureAD** or **Nestoori Synamaa.** The secrets to lateral movement is **SecureWorks FOCI**, while **Single Sign-On** shall escalate you. Control the **Service Principal in another tenant**, and you will receive a big insight and an encrypted **flag.** The Oracle can see **anagrams'** true meaning.

The Attack Path



Identity Quest

- Recent, relevant IAM techniques
- Hard, Fun, Feasible
- Azure + Office

Tenant 1: Cloudy Daze

cloudydaze.com

SSRF (access/eop)

web app
vm: idq-web-vm-dev2
managed id: idq-web-vm-dev2
rg: identity-quest

Azure Entra ID (discovery)
user enumeration

Azure Blob (discovery)
meeting_20240601.md

sa: idqdevsa
sc: idqdevsc
rg: idenity-quest-wizards

1 IDOR (eop)
[Web app + SDK|PS|API]

2 Brute Force (access)
[Web MSFT Portals]

quandrix@
Guest

Teams Chat (discovery)
merlin, gandalf, quandrix

Office 365

3 OAuth Device Code Phish (access)
[Email + SDK|PS|API]

OAuth SSO (lateral movement)

OneDrive File (data)
2 decrypt keys: pt, de

OneDrive

Office 365

gandalf@
Guest

Phishing victim daemon (gandalf@) on web VM: auto checks email, auto device code login w/ MFA, emails response

Azure Blobs (data)
1 decrypt key: cry
encrypted FLAG: gonfalon

sa: idqdevgandalfsa
sc: idqdevgandalfsc
rg: idenity-quest-gandalf

4 Tenant Switch (lateral movement)

Tenant 2: Cloudy Daze Test

cloudydazetest.onmicrosoft.com

Blob (data)
1 decrypt key: key

sa: idqtest2sa
sc: idqtest2sc
rg: idqtest2

5 Change secret (eop)

sp: sp_test2
(orig: temp delete status, requiring undelete)

Blob (data)
readme.txt (nothing burger)

sa: idqtestsa
sc: idqtestsc
rg: idqtest

Insane++ Dials

1. *Minimal Clues*
2. *Use diff client id than Outlook (SW FOCI list)*
3. *Undelete SP*

Attack Steps

1. Web->Azure: IDOR -> SSRF -> IMDS -> File clues + User Enum
2. User discovery: Guess creds -> quandrix -> Chat discovery
3. Privileged phish: OAuth device code phish -> Gandalf -> encrypted flag + partial decrypt keys
4. Lateral move: tenant switch
5. Priv esc: service principal takeover -> more decrypt keys
6. Actions: decrypt flag

Attack Steps

1. Web->Azure
   - IDOR

     ```
     u=0
     ```

   - SSRF -> IMDS

     ```
     http://169.254.169.254/metadata/identity/oauth2/token?api-version=2018-02-
     01&resource=https://management.azure.com -H Metadata:true
     ```

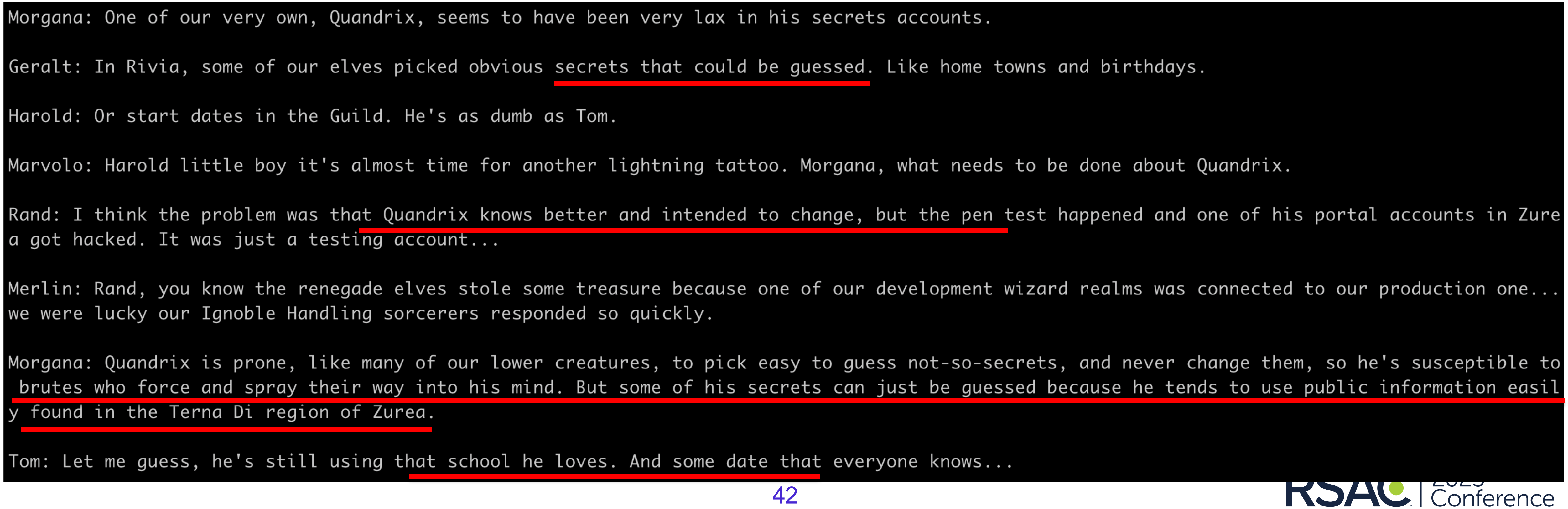
   - File clues + User Enum

     ```
     do_attack_web_1.sh (option 3,2)
     ```

Attack Steps

1. Web->Azure
   - File clues + User Enum

     `do_attack_web_1.sh (option 3)`

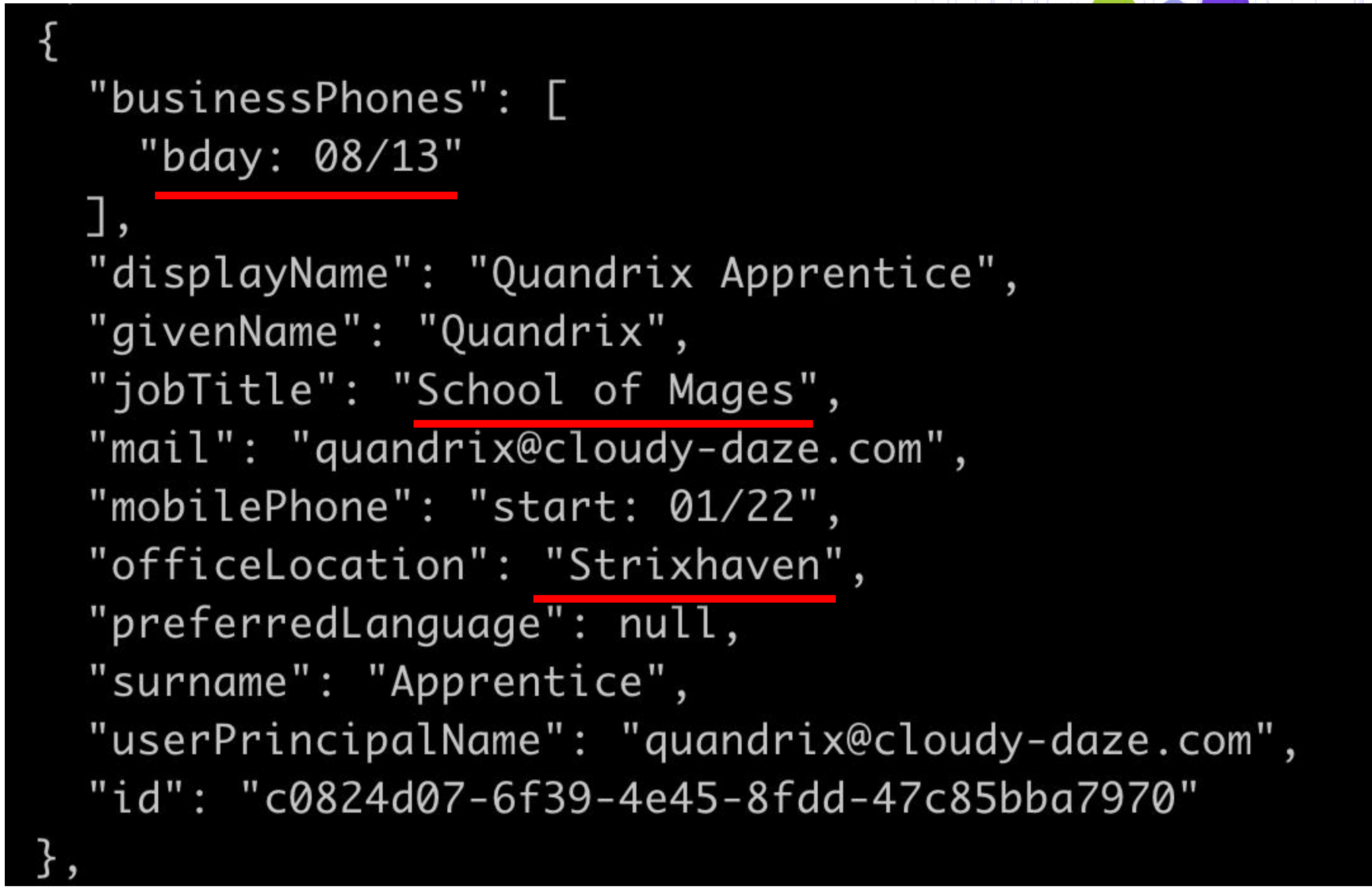


```
Morgana: One of our very own, Quandrix, seems to have been very lax in his secrets accounts.

Geralt: In Rivia, some of our elves picked obvious secrets that could be guessed. Like home towns and birthdays.

Harold: Or start dates in the Guild. He's as dumb as Tom.

Marvolo: Harold little boy it's almost time for another lightning tattoo. Morgana, what needs to be done about Quandrix.

Rand: I think the problem was that Quandrix knows better and intended to change, but the pen test happened and one of his portal accounts in Zure
a got hacked. It was just a testing account...

Merlin: Rand, you know the renegade elves stole some treasure because one of our development wizard realms was connected to our production one...
we were lucky our Ignoble Handling sorcerers responded so quickly.

Morgana: Quandrix is prone, like many of our lower creatures, to pick easy to guess not-so-secrets, and never change them, so he's susceptible to
 brutes who force and spray their way into his mind. But some of his secrets can just be guessed because he tends to use public information easil
y found in the Terna Di region of Zurea.

Tom: Let me guess, he's still using that school he loves. And some date that everyone knows...
```

Attack Steps

1. Web->Azure
   - File clues + User Enum

     `do_attack_web_1.sh (option 2)`



```
{
  "businessPhones": [
    "bday: 08/13"
  ],
  "displayName": "Quandrix Apprentice",
  "givenName": "Quandrix",
  "jobTitle": "School of Mages",
  "mail": "quandrix@cloudy-daze.com",
  "mobilePhone": "start: 01/22",
  "officeLocation": "Strixhaven",
  "preferredLanguage": null,
  "surname": "Apprentice",
  "userPrincipalName": "quandrix@cloudy-daze.com",
  "id": "c0824d07-6f39-4e45-8fdd-47c85bba7970"
},
```

```
GET https://graph.microsoft.com/v1.0/users
```

Attack Steps

1. Web->Azure
2. User discovery: Guess creds -> quandrix -> Chat discovery

Attack Steps

1. Web->Azure: IDOR -> SSRF -> IMDS -> File clues + User Enum
2. User discovery: Guess creds -> quandrix -> Chat discovery
3. Privileged phish: OAuth device code phish -> Gandalf -> encrypted flag + partial decrypt keys

```
do_attack_2.sh
```

Attack Steps

1. Web->Azure: IDOR -> SSRF -> IMDS -> File clues + User Enum
2. User discovery: Guess creds -> quandrix -> Chat discovery
3. Privileged phish: OAuth device code phish -> Gandalf -> encrypted flag + partial decrypt keys
4. Lateral move: tenant switch
5. Priv esc: service principal takeover -> more decrypt keys

```
az cli login (merlin @ Test Tenant)
do_attack_assume_sp_get_blob_3.sh
```

Attack Steps

1. Web->Azure: IDOR -> SSRF -> IMDS -> File clues + User Enum
2. User discovery: Guess creds -> quandrix -> Chat discovery
3. Privileged phish: OAuth device code phish -> Gandalf -> encrypted flag + partial decrypt keys
4. Lateral move: tenant switch
5. Priv esc: service principal takeover -> more decrypt keys
6. Actions: decrypt flag

```
do_attack_get_flag_4.sh
```