RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: CTF-T09

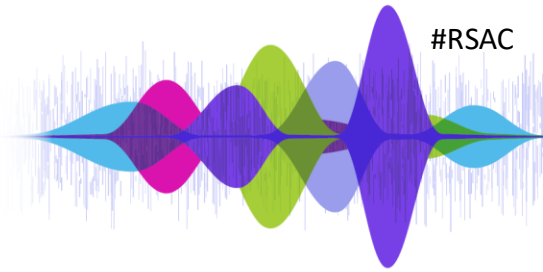
Cloud CTF 201: Solving Capture-The-Flag Challenges in AWS, Azure, GCP

Jenko Hwong
Threat Research
WideField Security

Luis Rivas
Network System Engineer
Department of Defense

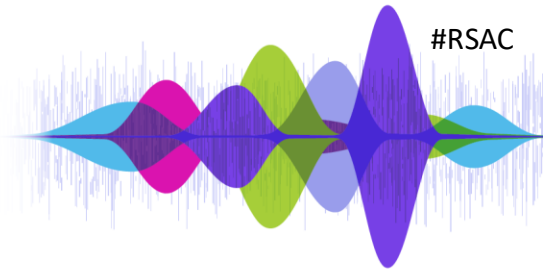
RSAC 2025 Conference

Azure Challenge Walkthrough



General

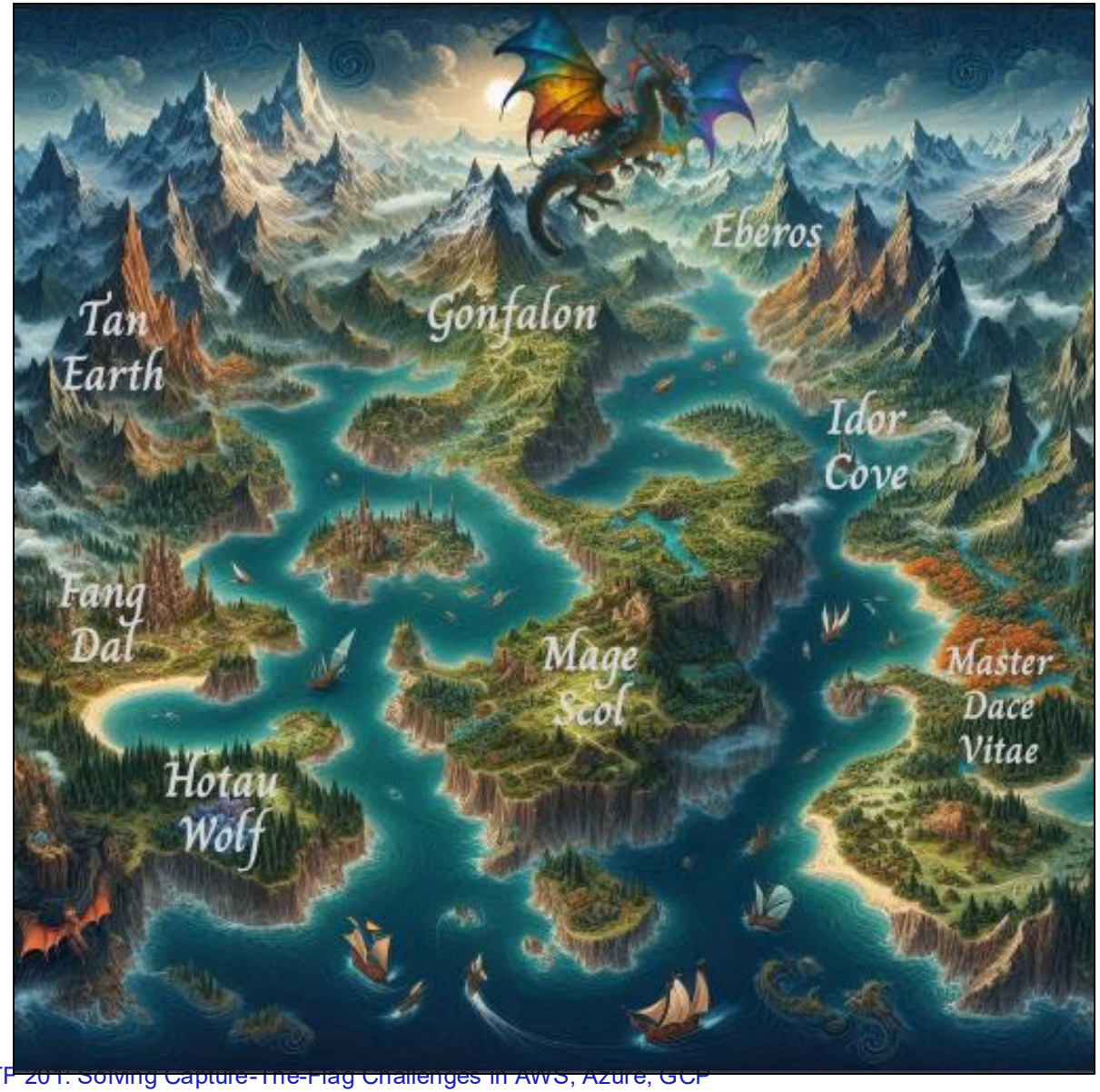
- Hard to Insane Azure Challenge
- Azure TTP focus
- Heavy game theme/puzzles (mixed)
- Tried to use recent real-world TTP
  - User **discovery**
  - OAuth device code **phish**
  - Microsoft SSO (Azure - Apps)
  - Lateral movement / stealth (tenant #2, **deleteItems**)



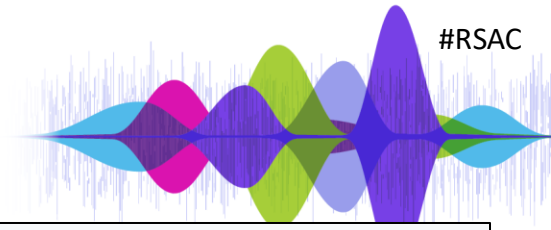
Starting point

- 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

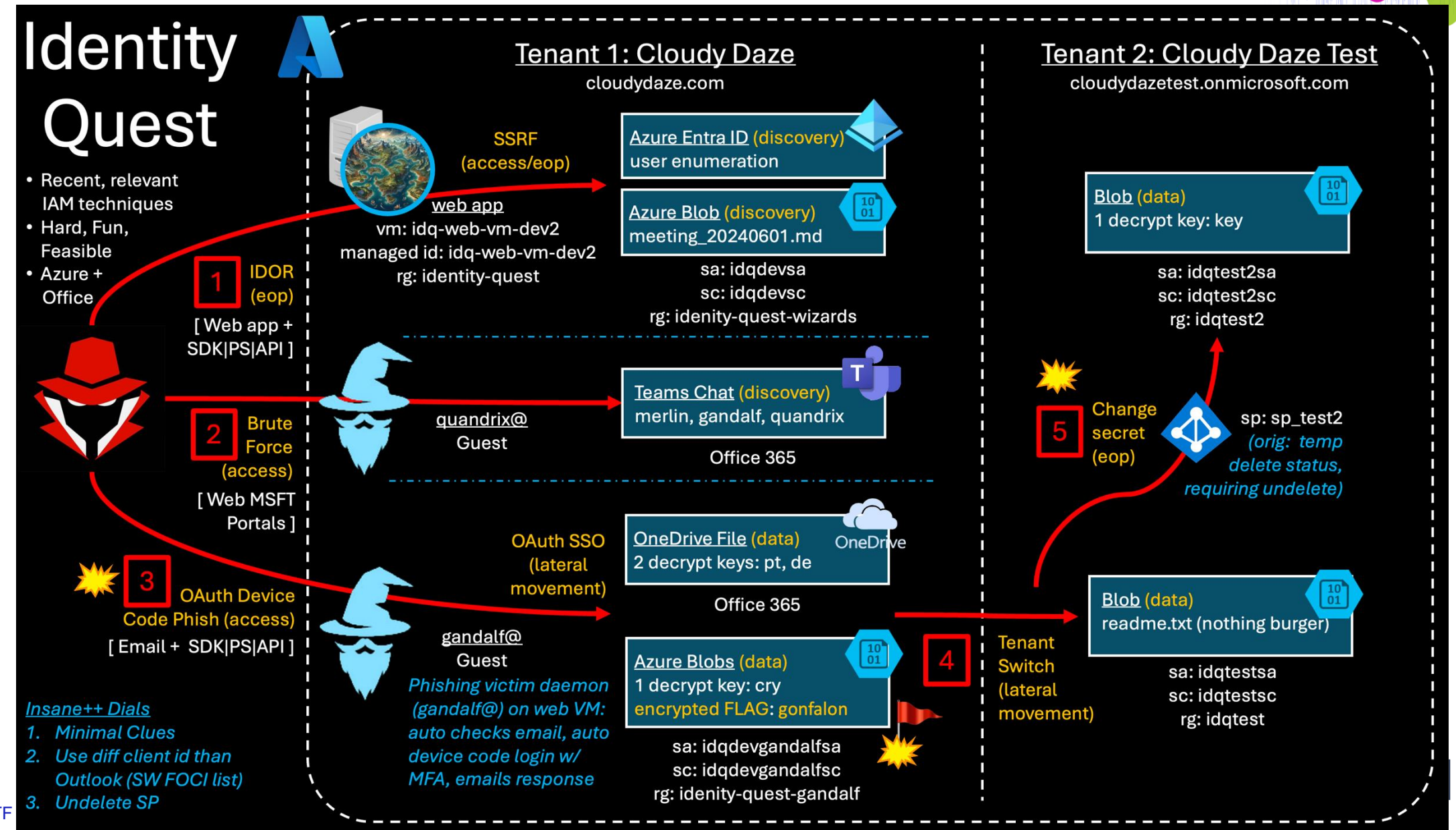


The Scroll

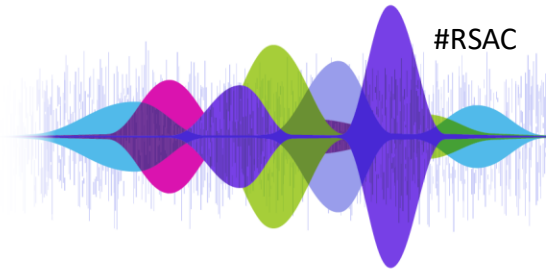
To cross the threshold into the cerulean skies of **Zurea Terna Di,** seek the **Novitiate's Pegasus Sword askew.** Then fathom how **the White's Hotau Wolf** can be **co-deceived.** The incantations thou requirest were cast by **Razed Dura** or **Anonymise Trio.** The whispered lore to askance traverse 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

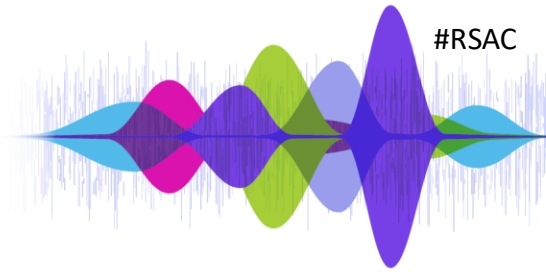


Attack Steps



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
     ```

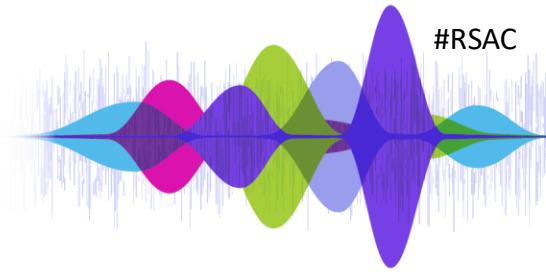
   - SSRF -> IMDS

     ```
     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...
```

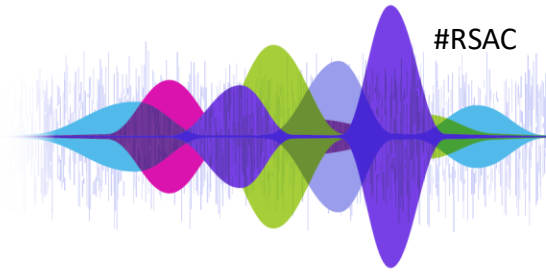
Attack Steps

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"
},
```

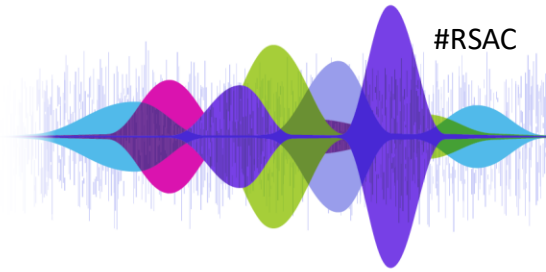

`GET https://graph.microsoft.com/v1.0/users`



Attack Steps

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

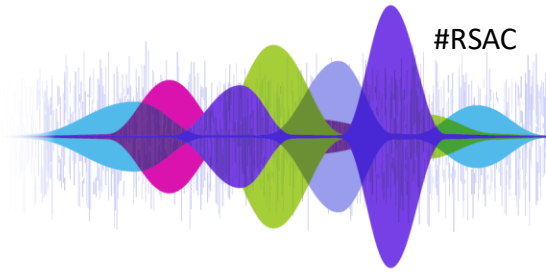
Attack Steps



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
```

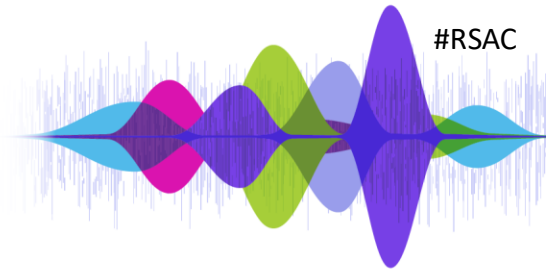
Attack Steps



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
```