What else can we do with this?

- Collect Info about user's setups
  - SDK and OS Version
  - What API's are called (awscli v2.0.36 and newer)
- Map out resources via CloudTrail logs

```
PUT /latest/api/token HTTP/1.1
Host: 169.254.169.254
Accept-Encoding: identity
x-aws-ec2-metadata-token-ttl-seconds: 21600
User-Agent: aws-cli/2.0.36 Python/3.7.4 Darwin/19.6.0 exe/x86_64 command/s3.ls
Content-Length: 0
```

The Details

It’s never that easy

- No default profile set
- No profile specified when run
- Attacker is on the local subnet
- Ugly errors

```
% aws s3 ls my-randomly-named-bucket-af83ne92h

An error occurred (NoSuchBucket) when calling the ListObjectsV2 operation: The specified bucket does not exist
```