Fake EC2 IMDS Server

Vs User Data Swap — Pros

- Does not require ModifyInstanceAttribute to the instance
- Can be quicker
- Our user data run’s before the real user data
  - cloud-init clean && reboot
- Impact is not obvious when looking at CloudTrail logs

Fake EC2 IMDS Server

Vs User Data Swap — Cons

- Breaks IMDS routing for the subnet for a short period of time
  - Likely will work best in subnet’s few, lightly used instances
- Difficult to troubleshoot
- Requires the attacker to be able to have full control over a single instance
  - Run’s against other subnet’s in the same VPC