Fake EC2 IMDS Server

Vs User Data Swap — Cons

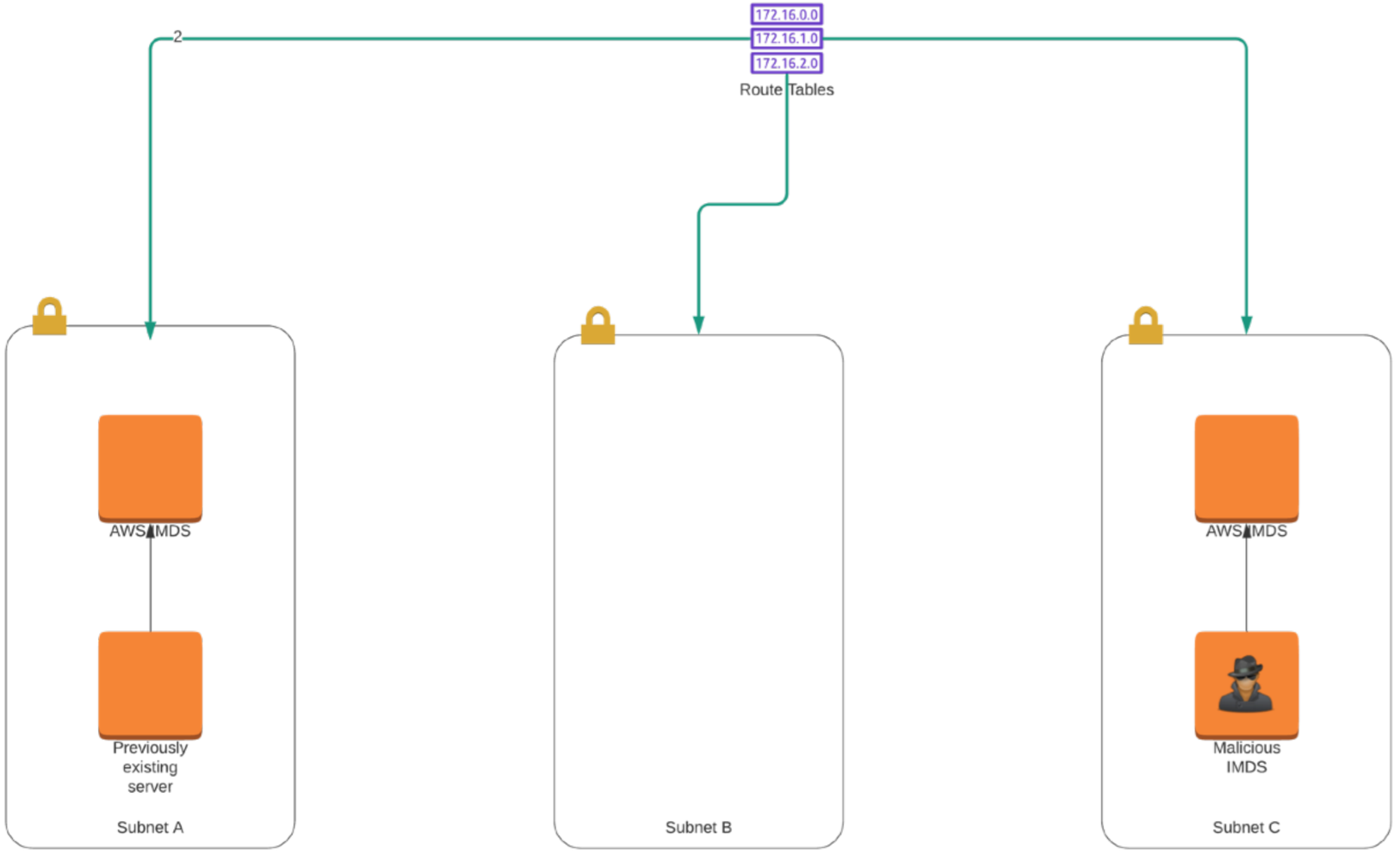
- Breaks IMDS routing for the subnet for a short period of time
  - Likely will work best in subnet’s few, lightly used instances
- Difficult to troubleshoot
- Requires the attacker to be able to have full control over a single instance
  - Run’s against other subnet’s in the same VPC

AWS IMDS Persistence/Priv escalation

Ryan Gerstenkorn | November 29, 2020

Default Routing

Use the tabs at the bottom to cycle between states.



Attacker Assumptions

- Controls an existing instance that has source IP checking disabled.
- Can modify routes
- Can trigger a lambda they control on RunInstance event's.

End Result

- New Instances in specific subnet's are automatically rooted on creation.

Notes

The key things that make this work.

- You can change what IMDS server a given instance connect's to by using a /32 route.
- Event Bridge is fast.
- Security groups are ignored for data to 169.254.169.254.
- No HTTPS w/ IMDS!