MITRE ATT&CK

MITRE ATT&CK has a cloud matrix representing tactics and techniques for cloud attacks. The page is located at https://attack.mitre.org/matrices/enterprise/cloud/. Using MITRE ATT&CK, we can plan our attacks from beginning to end before we start scripting. Some of the tactics and techniques we could use for example scenarios are:

- **Initial Access**
  - Drive-by Compromise
  - Phishing
  - Valid Accounts
- **Execution**
  - User Execution
- **Persistence**
  - Account Manipulation
  - Create Account
  - VAlid Accounts
- **Privilege Escalation**
  - Valid Accounts
- **Defense Evasion**
  - Hide Artifacts
  - Impair Defenses
  - Use Alternate Authentication Material
  - Valid Accounts
- **Credential Access**
  - Steal Web Session Cookie
  - Unsecured Credentials
- **Discovery**
  - Account Discovery
  - Cloud Infrastructure Discorvery
- **Lateral Movement**
  - Use Alternate Authentication Material
- **Collection**
  - Data from Cloud Storage Object
  - Data from Information Respositories
  - Data Staged
  - Email Collection
- **Exfiltration**
  - Transfer Data to Cloud Account
- **Impact**
  - Data Destruction
  - Data Encrypted for Impact
  - Defacement
  - Endpoint Denial of Service
  - Network Denial of Service

– Resource Hijacking