MITRE ATT&CK-Containers Matrix

ID:TA0001 Initial Access

- T1190 - Exploit Public-Facing Application
- T1133 - External Remote Services
- T1078 - Valid Accounts
  - Default Accounts
  - Local Accounts

ID:TA0002 Execution

- T1609 - Container Administration Command
- T1610 - Deploy Container
- T1053 - Scheduled Task/Job
  - Container Orchestration Job
- T1204 - User Execution
  - Malicious Image

ID:TA0003 Persistence

- T1133 - External Remote Services
- T1525 - Implant Internal Image
- T1503 - Scheduled Task/Job
  - Container Orchestration Job
- T1078 - Valid Accounts
  - Default Accounts
  - Local Accounts

ID:TA0004 Privilege Escalation

- T1611 - Escape to Host
- T1068 - Exploitation for Privilege Escalation
- T1053 - Scheduled Task/Job
  - Container Orchestration Job
- T1078 - Valid Accounts
  - Default Accounts
  - Local Accounts

ID:TA0005 Defense Evasion

- T1612 - Build Image on Host
- T1610 - Deploy Container
- T1562 - Impair Defenses
  - Disable or Modify Tools
- T1070 - Indicator Removal
- T1036 - Masquerading
  - Match Legitimate Name or Location
- T1550 - Use Alternate Authentication Material
  - Application Access Token
- T1078 - Valid Accounts
  - Default Accounts
  - Local Accounts

ID:TA0006 Credential Access

- T1110 - Brute Force
  - Password Guessing
  - Password Spraying
  - Credential Stuffing
- T1528 - Steal Application Access Token
- T1552 - Unsecured Credentials
  - Container API
  - Credentials In Files

ID:TA0007 Discovery

- T1613 - Container and Resource Discovery
- T1046 - Network Service Discovery
- T1069 - Permission Groups Discovery

ID:TA0008 Lateral Movement

- T1550 - Use Alternate Authentication Material
  - Application Access Token

ID:TA0040 Impact

- T1499 - Endpoint Denial of Service
- T1498 - Network Denial of Service
- T1496 - Resource Hijacking