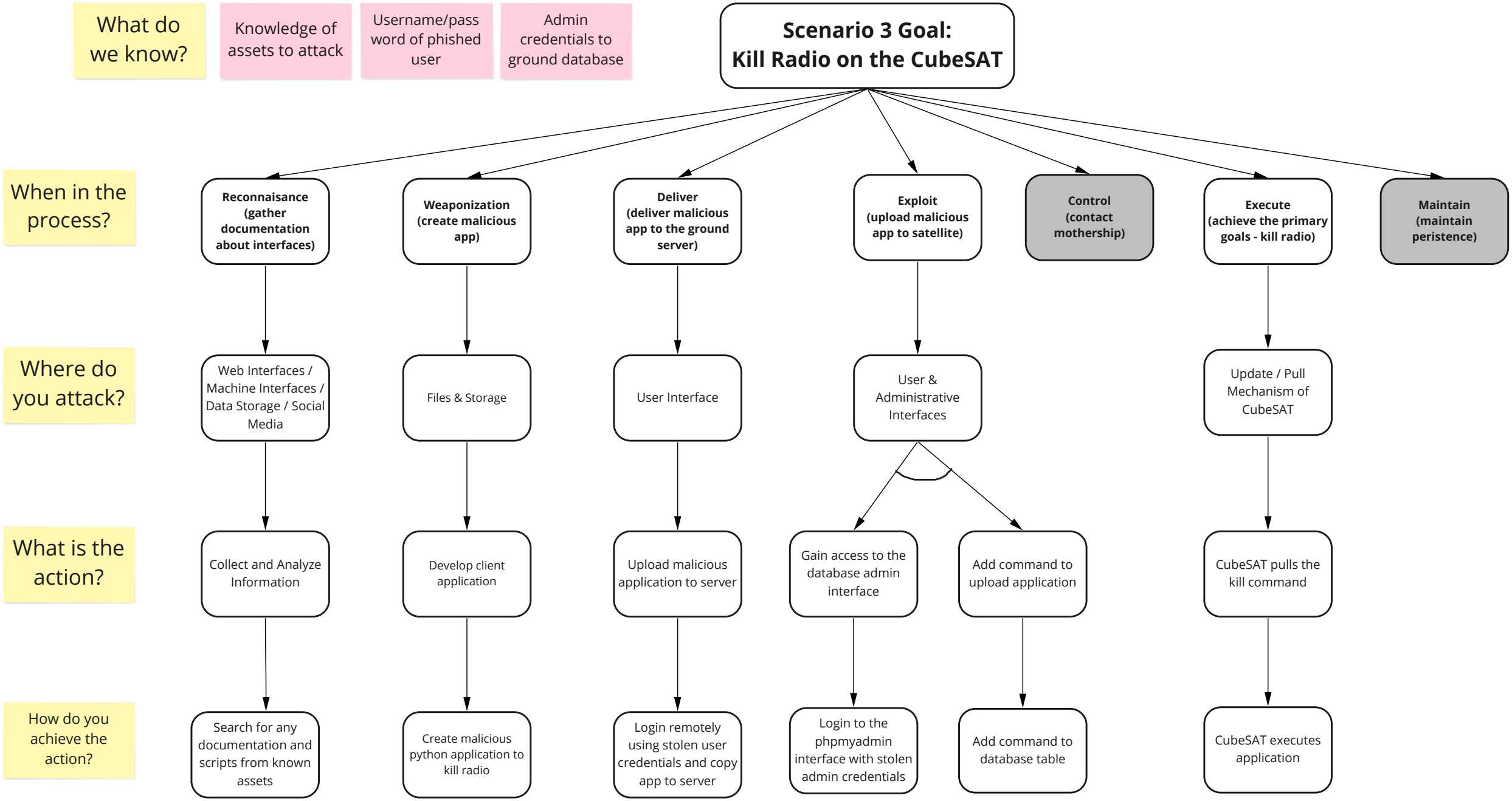
What do we know?
Knowledge of assets to attack
Username/password of phished user
Admin credentials to ground database
Scenario 3 Goal: Kill Radio on the CubeSAT
When in the process?
Where do you attack?
What is the action?
How do you achieve the action?
Reconnaisance (gather documentation about interfaces)
Weaponization (create malicious app)
Deliver (deliver malicious app to the ground server)
Exploit (upload malicious app to satellite)
Control (contact mothership)
Execute (achieve the primary goals - kill radio)
Maintain (maintain peristence)
Web Interfaces / Machine Interfaces / Data Storage / Social Media
Files & Storage
User Interface
User & Administrative Interfaces
Update / Pull Mechanism of CubeSAT
Collect and Analyze Information
Develop client application
Upload malicious application to server
Gain access to the database admin interface
Add command to upload application
CubeSAT pulls the kill command
Search for any documentation and scripts from known assets
Create malicious python application to kill radio
Login remotely using stolen user credentials and copy app to server
Login to the phpmyadmin interface with stolen admin credentials
Add command to database table
CubeSAT executes application