AI driven honeypots allow for an in depth study of attack signature behaviors. A honeypot allows for a system to experience and interact with bad actors in a controlled environment. In this project, we plan to use AI to:

1. deploy honeypots
2. Study weaknesses in different systems
3. Implement security measures based on the attacks
4. Visualize the various attacks graphically
5. Interact with bad actors to develop attacker profiles

Project Goal: Develop an AI agent to deploy dynamic high-interaction honey pots

Work Breakdown Structure

1. **Initiating**
   1. **Stakeholders**
      1. Honoore Mandiamy
      2. Loksharan Saravanan
   2. **Tools**
      1. Github
      2. AWS
      3. AI Generation Software
      4. Virtual Machines
         1. Kali Linux
         2. UBUNTU
      5. Networking tools
         1. NMAP
         2. HPING3
         3. NetStat
         4. Wireshark
2. **Planning**
   1. AI Agent
   2. Honeypots
   3. Network Penetration
   4. Paper and Presentation
      1. Research Goal - Creating an AI agent to develop dynamic, high-interaction honey pots to study attack signatures and attacker behaviors.
      2. Research Field - The honeypots will be geographically located in some of Amazon's Northeastern servers. The servers will be in the same region to simulate a local area network.
      3. Academic Background - IEEE reports, AWS documentation, ai generation report, and academic journals regarding honeypots ai agents and the tools used for this project.
      4. Background Research - City College professors and professionals in the tech industry.
      5. Scheduling
         1. Research
            1. 0/18 - 9/30
         2. Experimentation
            1. 10/1 - 11/14
         3. Results and Findings
            1. 10/17 = 11/25
         4. Project Conclusion
            1. 11/25 - 12/10
   5. Fieldwork
      1. Develop AI agent and honeypot frameworks
      2. Examine attacks from bad actors
      3. Implement security measures on honeypots
      4. Release harder to penetrate honeypot
   6. Collect and Visualize Data
      1. Use python matlab to generate graphs from experiment
   7. Report Findings
3. **Executing**
   1. Develop AI agent
   2. Create honeypot frameworks
   3. Release honeypots
   4. Penetrate honeypots with different attacks
   5. Implement security measures on honeypot frameworks
   6. AI agent releases harder to penetrate honeypots
4. **Monitoring/Reviewing**
   1. Analyze honeypot metrics on AWS and generate reports and graphs based on metrics
5. **Closing**
   1. This project provides the opportunity to gain a variety of technical skills from training an AI agent to implementing security measures against attacks many organizations suffer from today.