Hệ thống mô phỏng Attack-Defend trên không gian mạng là một giải pháp đột phá để luyện tập và cải thiện khả năng phòng thủ của các chuyên gia bảo mật mạng. Hệ thống này cho phép các chuyên gia bảo mật mạng tạo ra các kịch bản tấn công và phòng thủ trên môi trường gần với thực tế, giúp tăng cường khả năng phát hiện và ngăn chặn các cuộc tấn công mạng. Bên cạnh đó, hệ thống còn cung cấp một môi trường an toàn để luyện tập và nâng cao các kỹ năng cần thiết.

Đối tượng chính của hệ thống này là các chuyên gia bảo mật mạng và sinh viên học về an toàn thông tin có nhu cầu luyện tập và nâng cao khả năng phòng thủ trên không gian mạng. Bên cạnh đó, các tổ chức và doanh nghiệp cũng có thể tận dụng hệ thống này để kiểm tra và cải thiện khả năng phản ứng trước các cuộc tấn công mạng. Các thành phần cấu tạo nên hệ thống gồm: 1 Gateway, 3 Proxy, và máy tính cá nhân của các bên tấn công, phòng thủ. Gateway và 3 proxy servers sẽ được build trên docker.

Quy trình xây dựng hệ thống bao gồm:

* Thiết kế database
* Xây dựng server với các giao thức cần thiết
* Bổ sung các APIs
* Xây dựng các giao tiếp phía client
* Dựng hệ thống demo.

(Ref. [Destructive Farm](https://github.com/DestructiveVoice/DestructiveFarm))

Đối với sinh viên, hệ thống này sẽ là môi trường chất lượng để luyện tập và thử nghiệm các kỹ năng liên quan đến ngành học của mình. Đối với các doanh nghiệp thì đây là cơ hội để củng cố kinh nghiệm, cũng như tạo ra cơ hội học hỏi lẫn nhau giữa các nhân viên. Hiện nay cũng có một vài mô hình tổ chức mô phỏng tương tự, nhưng đối với dự án này, các quy trình quản trị và kết nối sẽ được tối giản để có thể dễ dàng làm quen, cũng như tập trung vào những vấn đề cốt lõi.