Cuộc tấn công từ chối dịch vụ (DoS), hay còn gọi là "Denial of Service" attack, là một hình thức tấn công mạng mà mục tiêu của nó là làm cho dịch vụ trở nên không khả dụng cho người dùng cuối bằng cách làm quá tải hệ thống hoặc gây ra sự cố với dịch vụ.

Trong một cuộc tấn công từ chối dịch vụ, kẻ tấn công thường gửi một lượng lớn yêu cầu hoặc dữ liệu không hợp lệ đến một dịch vụ hoặc máy chủ cụ thể, dẫn đến việc quá tải hệ thống và khiến cho dịch vụ không còn khả dụng cho người dùng hợp lệ nữa. Các dịch vụ mạng như website, ứng dụng web, máy chủ email và các dịch vụ trực tuyến khác đều có thể là mục tiêu của cuộc tấn công từ chối dịch vụ.

Các cuộc tấn công từ chối dịch vụ có thể được thực hiện bằng nhiều cách, bao gồm:

1. **Tấn công phủ nhận dịch vụ (DoS)**: Kẻ tấn công sử dụng một số phương tiện để làm quá tải hệ thống hoặc ứng dụng, làm cho nó không thể phản hồi cho yêu cầu từ người dùng hợp lệ. Ví dụ, kẻ tấn công có thể gửi một lượng lớn yêu cầu HTTP đến một trang web, khiến cho máy chủ web không thể xử lý tất cả các yêu cầu này cùng một lúc.
2. **Tấn công phủ nhận dịch vụ phân phối (DDoS)**: Đây là một dạng phức tạp của cuộc tấn công DoS, trong đó kẻ tấn công sử dụng một mạng lưới các máy tính được chiếm đoạt kiểm soát (botnet) để gửi yêu cầu đến một mục tiêu cụ thể. Sự phân tán của các yêu cầu từ nhiều nguồn khác nhau làm cho nó khó phát hiện và ngăn chặn.

Cuộc tấn công từ chối dịch vụ có thể gây ra hậu quả nghiêm trọng đối với doanh nghiệp hoặc tổ chức, bao gồm mất dữ liệu, gián đoạn hoạt động kinh doanh và hậu quả về uy tín. Để ngăn chặn và bảo vệ khỏi cuộc tấn công từ chối dịch vụ, các tổ chức thường triển khai các biện pháp bảo mật như tường lửa, giám sát mạng, và giải pháp chống DDoS.