Bài tập về nhà

- **B.1.1**

1. Đã làm trên lớp.
2. Staged và Non-Staged payload:

Stage payload là những payload có thên được phần cách bởi dâu '/', như windows/shell/bind_tcp. Trong khi đó Non-Staged payload là những payload có tên được phân cách bởi dấu '_', như windows/shell_bind_tcp.

	Staged Payload	Non-Staged Payload
Kích thước	Có kích thước nhỏ hơn Non-Staged payload, do Staged Payload chỉ gửi một stager nhỏ đến máy nạn nhân, stager này có nhiệm vụ kết nối ngược lại đến máy attacker và download các phần payload cần thiết.	Có kích thước lớn, do Non-Staged Payload gửi toàn bộ payload cần thiết đến máy nạn nhân chỉ trong một lần duy nhất, vì vậy nó không yêu cầu attacker cung cấp thêm bất kì dữ liệu nào nữa.
Công cụ lắng nghe kết nối	Do Stage payload cần download thêm các payload khác từ attacker nên nó cần 1 bộ công cụ lắng nghe đặc biệt như multi/handler trong Metasploit.	Do đơn giản hơn Stage Payload, nên Non-Stage Payload có thể sử dụng nhiều công cụ lắng nghe khác nhau, như Netcat.
Khả năng phát hiện của các phần mềm anti-virus	Khó phát hiện hơn so với Non-Stage Payload, do có kích thước nhỏ -> dễ che dấu	Dễ bị phát hiện

3. link youtube: https://www.youtube.com/watch?v=UAKJOZM4duQ

- **B.2.2:**
    1. Link youtube: https://youtu.be/_IvYFngigU0
    2. So sánh giữa việc nhúng payload vào tập tin và tạo payload mới:

	Nhúng payload vào tập tin	Tạo payload mới
Kích thước	Lớn hơn so với việc tạo payload mới vì phải gắn vào tập tin khác	Có kích thước nhỏ
Khả năng phát hiện bởi người dùng	Khả năng bị phát hiện thấp do được cải trang thành một tập tin bình thường -> khả năng người dùng kích hoạt tập tin sẽ cao hơn	Dễ bị phát hiện do đứng độc lập