Each 6.1800 lecture will come with an outline. You can fill this in during lecture, after lecture, or not at all — it's entirely up to you how you use it. The goal of these outlines is to help you understand the main points that you should be taking away from each lecture. In some cases we will also include examples of things you should be able to do after each lecture.

In the past, these outlines have proved to be an effective tool for studying for the exams. Note that the outlines are ***not exhaustive****; there will be topics and nuances in lecture that aren't captured by the outline.*

Lecture 25: DDoS attacks

- What is the purpose of a DDoS attack? (i.e., what is the adversary trying to do?)
- What are some ways that machines can become part of a botnet?
- How are botnets typically structured?
- How do the two approaches to Network Intrusion Detection Systems (NIDS) compare?
    - Why don't such systems perfectly prevent DDoS attacks?
- You'll see four examples of attacks in lecture. How do they each work? Specifically:
    - What does the adversary do in each attack?
    - What resource is exhausted? (network, disk, etc.)
    - What makes the attack hard to detect/prevent?