1A Assuming our challenge r returns the same number of bits each time (sha-256 for example) we can determine the probability of the last n bits being zero via the following equation. (2^256-n)/(2^256) We are assuming that each bit is generated randomly. On average the client will have to perform the hmac around (2^256-n)/(2^256) times. The server simply verifies the clients solution, so it will perform the hmac once.

1B If we wanted to negate an amplification factor of 64 then the we want the client to calculate the hmac 64 times more than the server. To do this we can see that 64 = 2^6. We can then require the last 6 bits to be 0 on the solution the client returns. This means the client has (2^256-6)/(2^256) or 0.0156 probability of guessing a working solution. Using the combinatorics equation of (64\*0.0156)-(0.0156^64) we can see that after 64 attempts the client has about a 100% likelihood of getting a correct solution.

2A A low orbit ion cannon works by adding users who download the software to a network, and then pointing every machine in that network to a certain web server online. The main mechanism fires off random requests as quickly as possible using sockets and threads. This gets as much traffic from each machine as possible, and when combined has the power to cause the server to fail.

2B Hive-mind mode connects your machine to an IRC server that allows it to be controlled remotely. You basically add yourself to a botnet that does not allow remote administration of your client, but sends packets from your client. As the admin of the LOIC you can send a message specifying the target IP, the message, and the protocol. You can also start and stop the attack at your digression.

2C The first step in defending against LOIC attacks is to detect network anomalies as quickly as possible. Intrusion prevention/detection system alarms can be installed at strategic points in the network, and help to notify the organization of malicious users and trigger action. One way to determine bots from users is to use access control lists. ACLs have requirements that each packet must meet, and if the packet doesn’t meet one of the requirements it can deny it.

2D Operation Payback was a movement from piracy advocates and Anonymous in retaliation to the DDOS attacks on torrent sites. It also included DDOS attacks on financial institutions that stopped working with WikiLeaks such as Visa, and MasterCard.

2E Christopher Wayne Cooper was a hacktivist that partook in Operation Avenge Assange, and helped to attack PayPal after they stopped forwarding donations to WikiLeaks. The charge he faced was conspiracy to commit intentional damage to a protected computer. He and several other members of Anonymous conducted a DDOS attack.

2F LOIC Hive Mind mode is different than a typical botnet in that users decide to join the botnet, and give permission for their machine to be used in the DDOS attack. LOIC still performs a DDOS attack in a similar method as any other botnet.

2G LOIC hive mind mode is similar to a political protest because clients can choose to be part of an attack just like a protestor can choose to join a protest. They differ in that many political protests are legal gatherings and peaceful, LOIC is not peaceful and is intended to disrupt service maliciously.