PRANITA CAMASAMUDRAM

MID TERM-1

1. Explain what a DDoS amplification factor is and how to measure it.
Ans : A DDoS amplification factor is the ratio of the victim's response measure size and the request message size that the service provider received. For the attacker the largest amplification factor is ideal. Few of the examples are Memcached which has upto 51200 whereas NetBios only has 3.85 [1]. The factor also depends on the number of IP addresses returned by the server.

2. Describe an influential DDoS attack that happened in the last 20 years. Explain how it was influential.
Ans : One of the ddos attacks that I consider as influential is the one that happened between Estonia and Russia in 2007. As Estonia was the most internet connected country at the time, it was especially left vulnerable. With the attack reaching 4 million packets per second, the economy was hit so badly that the government, schools, hospitals,media etc were shut down for weeks. The government, after knowing that an outside source is responsible for such an attack, it secluded the internet from the rest of the world. I do consider it as influential because it is considered as the first "cyberwar" between two countries and showed the world how important national security for the internet is.

3. How good is simulated DDoS attack traffic for modeling and understanding DDoS activities?
Ans : Simulated traffic is definitely not the same as actual attack traffic. I feel that simulated attacks give a really good sense of how the user or network works when an attack is made as I have learnt through the lab assignments. But the packets in simulated attack is way less than what a real attack will have. This is no good for anticipating the situation where millions of packets are being sent every second. Sure it may have a good amplification factor, but still it is far fetched to say it will give a good understanding of complex DDoS activities.

4. Explain how botnets work and their influence on DDoS.
Ans : Botnets are created in order to accept commands and updates so that they can perform attacks on the network and expand more bots if they find any more vulnerable hosts. Botnets first start off with infecting the target eg., spam emails, sharing files. Then the code runs to download botnet binaries. Once the binaries

are downloaded and executed, the bots are established. These binaries can communicate with a CnC network, so the work of newly formed bots is to discover these networks and connect to them. Thai is so that they can stay connected to the botnet all the time. After this the bots execute the commands coming from the CnC network to perform malicious activities. Due to this CnC network they come up with a wide range of architectures to perform DDoS attacks. Botnets, today are the largest and widely coordinated DDoS attacks performed.

5. How effective are anti-DDoS laws? Why? Is this primarily a legal, technical, or social issue?

Ans : The anti-DDoS laws depend on country to country and situation to situation. From the upper layer, all DDoS attacks are illegal. But as we dig deeper we find much more complicated situations. Anti-DDoS laws definitely protect individuals from major cybercrimes or at least punish the ones responsible for it. But when it comes to activities that are done as a part of "activism" need more depth and understanding. As long the protests are non violent and limited to peaceful protests without damaging huge chunks of the economy, the laws can be slacked as exceptional cases. As for what issue they are, I would say first it is a legal issue. A lot of DDoS attacks include real legal risks. Especially when the military is involved. I would say that protecting legal laws is important for even "hacktivists" as cybercrime can be as elaborate as shutting down countries. Then comes social and technical issues which should be evaluated as per the situation.