CS6500

Reading Assignment - DDoS Attacks

Sanjana Prabhu EE17B072

March 15, 2021

DDoS attack or distributed Denial-of-service attack is a type of network security attack wherein the attacker tries to disrupt traffic of a user by flooding the network with a lot of unwanted traffic. Due to the huge amount of traffic that creates a load on the network core, the user is not able to access the network services and resources as desired. Therefore, the "Availability" aspect of security is compromised.
The earliest documented DDoS attack occurred in February 2000, when a 15-year-old Canadian hacker, launched DDoS attacks against several websites, including Amazon and eBay. The largest DDoS attack till date was in February 2020, when Amazon Web Services was flooded with 2.3 Tb/seconds of network traffic. In the past, DDoS attacks have mostly been carried out on servers having sensitive data such as credit card and payment servers.
The mechanism behind DDoS attacks is that the attacker gets control over a large number of devices connected to the Internet - these are called bots. These bots can then be used to do whatever the attacker intends to, such as send malware to the target or flood the target server with request and enable as DDoS attack. In the ever expanding IoT(Internet-of-Things) network dependent world, these kind of attacks are quite common, due to the way in which DDoS attacks are carried out, for example, the recent Dyn DDoS attack was orchestrated using IoT devices.
The DDoS attacks can be carried out by exploiting a number of vulnerabilities. One such vulnerability is the Telnet protocol vulnerability. Telnet protocol allows remote access by creating a virtual terminal, and it does not allow encryption. This security flaw lets the bots connect to the target server without user login credentials.
To mitigate DDoS attacks, a combination of detection, traffic classification and response tools are used. One of the techniques includes having a firewall which merely blocks incoming traffic from attackers, identified based on IP addresses, protocols and ports. In other techniques, vulnerable ports could be blocked such that a certain type of traffic cannot enter them, such as blocking incoming UDP traffic on port 1900 in an SSDP reflection attack.