Computer science

Technology, Information Technology

COMPUTER SCIENCE Dos/DDos Dos attack ification is vital in understanding the attacked protocols so as to avoid the worms on suitable platforms. Over the last decades there has been no study on the DDos attacks and therefore there is not much understanding on the same. This is because there is insufficient data at the backscatter. According to Kumar, there are some articles that have scrutinized the hosts that have been contaminated with the worms. This has been done through examination of the structure and the properties of the worms. This has been instrumental in the classification. Mandia and Prosise categorized the DDos attack into three distinct groups. These groups include Destructive, Resource consumption, and Bandwidth consumption attacks. On the other hand, Douligeris and Mitrokotsa advanced the classification to five groups which included Network OS level, Device level, Application level, Data flood, and Protocol feature attack. This can be explained below:

1. Bandwidth-based attacks

This often attacks the routers, servers and firewall processing resources and thus limiting them. Normaly, this type of DDoS attacks sent a lot of data which leads to an overload making the network brandwidthto be depleted. There is reduction in the quality of service when there is an overload attack in a system. This is because the normal access is tempered with.

2. Traffic-based attacks

This kind of attacks often sent large traffic attacks in form of TCP, UDP and other ICPM. Often people use technology forgery to escape the system monitoring. When the attacks are mixed with the malware exploitation, they cause leaking of the information and this may be dangerous. This illegal activity of information leakage will occur while fighting the DDoc attacks.

3. Application-based attacks

This is vital as it is used in the financial institutions to prevent breaches and leakages of the information. Though the attackers may not be many, this attack is taken for specific roles such as cancelling fraudulent transactions or accesses a vital database. (Chai, 2013)This often involves targeting application layer of OSI model. Normaly, application layer data is sent to the attackers to disable their functions.

4. Modus Operandi

Here, there is the involvement of a machine which in most cases are the agents. When the orders are received from the master machine which is controlled by the attacker, this agents will be involved in remitting the packets to a host who is a victim of the attack. The agents and master will then generate an actual attack message instructing the modus operandi to attack the network victim.