[Your Name]

[Instructor Name]

[Course Number]

[Date]

Network and Server Security

A Denial-of-Service (DoS) attack is a term used to define a cyber-attack that intends to halt a network, rendering it inaccessible to the legitimate users (Rengaraju, 2). A DoS attack is initiated by sending a flood of traffic to the target or giving it any information that causes it to crash (Rengaraju, 2).

For years, DoS attacks have been witnessed. However, some of the DoS attacks that did the rounds on the media are discussed ahead. In February 2018, GitHub fell victim to the DoS attack. GitHub is a famous platform where individuals share open-source editable source code. The recorded traffic was 1.35 terabits per second. In 2014, another massive attack rocked Occupy Central; a Hong Kong based democratic movement (Rengaraju, 2). The traffic that was recorded peaked to 500 gigabits per second. During the same year, a famous security provider, CloudFlare, was attacked with the incoming traffic recorded at 400 gigabits per second. During the year 2012, a chain of banks in the US was attacked. There were 5 banks were targeted in this attack with 60 gigabits of traffic per second flooding hundreds of servers of these banks.

There are certain ways through which a DoS attack can be prevented. The primary step that any organization can undertake to secure itself from the DoS attacks is to buy more bandwidth (Rengaraju, 3). It will help in comfortably handling the increased traffic sent from hackers. Another way to prevent DoS is to ensure that all the information of an organization does not reside on a single server (Rengaraju, 4). Furthermore, organizations can configure their network hardware to put up a strong resistance against the DoS attacks. Furthermore, specific web application firewalls can be used by organizations to make it tougher for hackers to breach in their systems.

Works Cited

Rengaraju, Perumalraja, V. Raja Ramanan, and Chung-Horng Lung. "Detection and prevention of DoS attacks in Software-Defined Cloud networks." *2017 IEEE Conference on Dependable and Secure Computing*. IEEE, 2017.