week 4 task 2

A slowloris DDoS attack works so that the threat actor forms many simultaneous tcp connections to the target server, computer or something similar, and then generates low volumes of HTTP requests from all the the simultaneous tcp-connections. This attacks allows the threat target to take down a web server with little effort and complexity.

a slowloris DDoS attack is unique because it doesn't require nearly as much resources as the traditional DDoS attacks, which are done by flooding the targeted server with overwhelming number of HTTP requests. Slowloris attack only requires a few hundred requests at different types of intervals. Slowloris attacks is also hard to detect compared to traditional ddos attacks due to the slow requests compared to traditional ddos attacks.

The effect of the attack is usually that it takes down a web server or the targeted device.

The slowloris attack can be mitigated by for example increasing the minimum amount of requests made to the server, limiting the amount of connections a single ip address can form, making a limit to the time a connection can be held by a client and using possible firewalls and other applications that can prevent the attacks.

One notable example of this attack was in 2009 against the Iranian government sites after the presidential election.

sources: https://www.cloudflare.com/learning/ddos/ddos-attack-tools/slowloris/, https://www.invicti.com/learn/slowloris-attack/, https://www.myrasecurity.com/en/knowledge-hub/slowloris/.