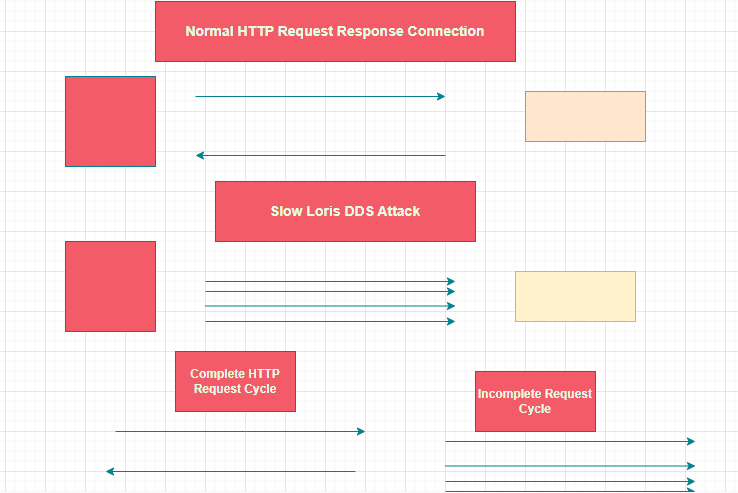
It is a denial of service attack (CloudFare, n.d.) in which the attacker targets the web server to make it unavailable to legitimate users. This attack program works by making many partial connections between the web servers and keeping those connections open for an extended period of time. It mainly focuses on typing up the server instead of overwhelming it with traffic. It is a specific track tool that takes down a server without using much bandwidth, unlike the high bandwidth consuming reflection-based DDoS attacks, and it is not a type of attack; instead, it is a specific track attack tool, and it falls in the category of low and slow attacks. The block diagram represents the slow Loris attack on a web server.



* It does not primarily depend upon heavy traffic like the traditional DDoS attacks and focuses on exploiting the web server by establishing multiple connections.
* It sends partial HTTP requests to make the connections seem genuine.
* Slow Loris sends small quantities of extra data regularly to keep these connections open, establishing multiple connections with the targeted server.
* It is hard to detect as it does not generate an immediate high traffic volume.

Following are the effects of slow Loris attacks.

* It can lead to slow response time for the original user and even make the server nonresponsive.
* A rise in the amount of CPU and open connections on the server.
* It can cause interruptions in the service and temporary outages.
* To prevent slow Loris attacks, the following steps should be taken.
* Limit the number of simultaneous connections from a single IP address.
* Use the DDoS protection tools and services
* Updates the software and security regularly.
* Set a server connection time-out rate.
* Use the software to monitor the traffic patterns to detect odd traffic.

After the Ukrainian war (Groves, 2023), a huge amount of such attacks were conducted on Ukrainian-based systems, which were majorly state-sponsored. In the last 5 years, there has been a huge increase in such attacks, especially in the two years of the pandemic, and many corporate organizations have been victims of such attacks. One famous attack (Anon., 2016) was “The Mirai Krebs and OVH DDoS Attacks in 2016,” in which more than 60000 IoT devices were compromised, and it has recorded 269 DDoS attacks since July 2012. Back in 2009 and 2010, Government websites were targeted by slow Loris attacks, and there have also been attacks against e-commerce websites. Frequently, these attacks try to interfere with services or make political statements.

# References

Anon., 2016. *Geoff Blaine.* [Online]   
Available at: https://www.a10networks.com/blog/inside-the-mirai-malware-that-powers-iot-botnets/  
[Accessed 05 10 2023].

CloudFare, n.d. *Cloud Fare.* [Online]   
Available at: https://www.cloudflare.com/en-gb/learning/ddos/ddos-attack-tools/slowloris/  
[Accessed 05 10 2023].

Groves, P. N. a. R., 2023. *a10networks.* [Online]   
Available at: https://www.a10networks.com/blog/systems-strike-ukraine-with-amplification-and-drdos-attacks/  
[Accessed 05 10 2023].