The Slow Loris Attack

It's a protocol attack(application layer), doesn't need a lot of bandwidth.

Slow loris are very slow animals, they are that slow that they may seem to appear as if you were watching a video in slo-mo.

When you open-up your web browser and enter a URL, you are basically communicating with a computer(called the server) and making few GET request over HTTP, like get me index.html server responds and that's the end of the conversation, and between two request sent from the attacker there are two new lines and as part of the firewall of the server - there is a time out counter that keeps the track of request and when to break the connection, what slow loris does is it basically establishes the connection, requests something from the server then it goes to sleep for few seconds and then when server is just about to break the connection because of the time counter the slow loris attacker send something more, it could be anything just to tell the server that I'm still here, doing so the the socket through which the server and the attacker were communicating is withheld for a very very slow computer, listen to the conversation of computer that is too slow to but yet taking the equal amount of resource as a normal user and imagine what if we have hundreds of the these socket occupied! the server will keep on serving those computers that are too slow that you may call them Slow Loris, it could break the server and the server won't be able to serve a legitimate

request so it can be called as a denial of service attack. And the beauty of this attack is this that it only occupies only the fraction of bandwidth of the attacker and compared to other DOS attacks it's a plus point for the attacker and these kind of attacks are very hard to detect because there is nothing wrong with these requests, it will appear to the server that those requesters have a really bad internet connection and that's perfectly normal. This attack is more prone to apache web server because it makes a new thread for a new request and what apache has is a limit on concurrent connection this system will work perfectly fine if the request comes and goes. And that's the point that slow loris exploits and what makes it the *Slow Loris.*