DDos (Abstract)

Mersed Keco, 4AHITN 2020/21

In this research paper we will answer what an DDoS attack is, the functionality of those attacks, different ways of DDoS attacks, how someone can protect himself from an attack and also the legal situation. This work was done mostly with the help of internet research.

Internet attacks are becoming a growing problem with the ongoing digitalisation. Phishing, ransomware, and DoS attacks are becoming more frequent every day and continue to grow in popularity. The special form of DoS attack, that we will talk about, is DDoS. It is not only used in important sectors for instance, network communication and healthcare, is mainly run to disturb or shut off a server and other appliances, mostly using the SYN-flood method and being using a bot-network. Due to the many ways of performing an DDoS attack, it is not an easy way of finding out the source and immediately react to the threat of maybe losing not only money, but also your nerves. That is why a lot of domain owners and companies hire DDoS specialist, who have the knowledge how to respond to such an attack and the needed infrastructure, because defending yourself can be tough without the knowledge. The legal consequences that follow if someone gets caught performing a DDoS attack or unknowingly being part of it, differentiate from the intention and the prior technical knowledge. Basically, it can start from only being a booking, a monetary fine but also going up to a prison sentence up to 40 years. The prison sentence turns out differently in every country because there is no standardized law according to this cybercrime.