ABSTRACT

Denial of Service (DOS) and Distributed Denial of Service (DDOS) are some methods to attack any kind of computer-based service, this method recently being used to bring down a web server of some multicultural organization, The primary target of this kind of attack usually exploiting layer 7 from OSI layer model, such as HTTP, FTP,SMTP and so on. This kind of service becomes a vital object for our digital lifestyle to accessing any content whatsoever, anywhere, anytime via internet, subscriber who accessing this kind of service isn't only one, there are millions, even billions of subscribers accessing this kind of service on internet everyday, so network security is a must.

In this final project, there will be a virtual network that's being designed for implementing the layer 7 DOS and DDOS attack simultaneously, then there's a web server that become the victim for this attack, to prevent the attack entering our server, there will be some kind of unpenetreable defense that monitoring our virtual network, considering that the attacks exploiting the HTTP header, so our defense (called Snort) will sort the packetst and differentiate the usual HTTP request packet and the HTTP packet that being used for attacking the web server, this task will be accomplished if snort has been configured to implementating NIPS deployment, NIPS itself (Network Intrusion Prevention System) is a some method to locating our defense system, when the DMZ area are in-line with the defense system. This final project needs some software for many things, including hypervisor for creating the virtual network, Ubuntu Linux to make the defense and web server, Kali linux for the attacker.

There are 1.063.713 attacks that have been thwarted with NIPS Snort defense system, 98 % of attack percentage comes from Torshammer with critical severity, also loads given from the attack is more plentiful if compared with the first attack, Nmap HTTP Brute Force, which is up to 40 %

Keywords : DOS, DDOS, Web server, NIPS, Snort, Ubuntu, Kali Linux