Contribution ID: **30** Type: **Paper presentation**

Network Congestion Solution for FTP Services Based on Distributed Firewall and Snort

Friday 16 September 2022 10:20 (20 minutes)

The exploit of network traffic has become common due to the increased flow of web traffic from services like HTTP, FTP, SMTP etc. The number of cyberattacks has grown due to the fact that they require different information about a target with the purpose of intimidating, blackmailing or harassing a person or a company. Servers of medical and dental organizations have become a good source of information for cyber criminals, due to the huge information stored across years. Besides compromised health data, another problem with huge impact is the congestion of a network. If a network of database servers is overcrowded, the result is high delays in obtaining the information of a patient that needs urgent medical care. In this paper, we are going to analyze network traffic generated by a network simulator during a User Datagram Protocol (UDP) flood. We are proposing a solution to this type of network attack, consisting in a custom firewall rule, that obtains significant improvements in the network resources usage. This paper specifically demonstrates the attack of LOIC on an FTP server inside a network that is managed by pfSense as firewall and Snort as IDS. We concluded the paper with the results of our study and the solution that we developed. Our study regarding this problem consists in an approach to solve the problem of the UDP flood inside a local network and also using open-source distributions to resolve the congestion of the network traffic.
Keywords—FTP, eHealth, Medical care, Snort, pfSense, UDP flood, vsftpd, IDS.

Author: TUDOSI, Andrei-Daniel (USV)

Presenters: TUDOSI, Andrei-Daniel (USV); GRAUR, Adrian; BALAN, Doru (USV); POTORAC, Alin Dan

Session Classification: Session 1A - Cloud Computing and Network Virtualisation

Track Classification: Cloud Computing and Network Virtualisation