World Academy of Science, Engineering and Technology
International Journal of Mathematical and Computational Sciences
Vol:14, No:12, 2020

Tracing Back the Bot Master

Authors : Sneha Leslie

Abstract : The current situation in the cyber world is that crimes performed by Botnets are increasing and the masterminds (botmaster) are not detectable easily. The botmaster in the botnet compromises the legitimate host machines in the network and make them bots or zombies to initiate the cyber-attacks. This paper will focus on the live detection of the botmaster in the network by using the strong framework 'metasploit', when distributed denial of service (DDOS) attack is performed by the botnet. The affected victim machine will be continuously monitoring its incoming packets. Once the victim machine gets to know about the excessive count of packets from any IP, that particular IP is noted and details of the noted systems are gathered. Using the vulnerabilities present in the zombie machines (already compromised by botmaster), the victim machine will compromise them. By gaining access to the compromised systems, applications are run remotely. By analyzing the incoming packets of the zombies, the victim comes to know the address of the botmaster. This is an effective and a simple system where no specific features of communication protocol are considered.

Keywords : bonet, DDoS attack, network security, detection system, metasploit framework
Conference Title : ICSRD 2020 : International Conference on Scientific Research and Development
Conference Location : Chicago, United States
Conference Dates : December 12-13, 2020