World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:15, No:12, 2021

Attack Redirection and Detection using Honeypots

Authors : Chowduru Ramachandra Sharma, Shatunjay Rawat

Abstract : A false positive state is when the IDS/IPS identifies an activity as an attack, but the activity is acceptable behavior in the system. False positives in a Network Intrusion Detection System (NIDS) is an issue because they desensitize the administrator. It wastes computational power and valuable resources when rules are not tuned properly, which is the main issue with anomaly NIDS. Furthermore, most false positives reduction techniques are not performed during the real-time of attempted intrusions; instead, they have applied afterward on collected traffic data and generate alerts. Of course, false positives detection in 'offline mode' is tremendously valuable. Nevertheless, there is room for improvement here; automated techniques still need to reduce False Positives in real-time. This paper uses the Snort signature detection model to redirect the alerted attacks to Honeypots and verify attacks.

Keywords : honeypot, TPOT, snort, NIDS, honeybird, iptables, netfilter, redirection, attack detection, docker, snare, tanner
Conference Title : ICCNS 2021 : International Conference on Communication and Network Security
Conference Location : Dubai, United Arab Emirates
Conference Dates : December 20-21, 2021