Abstract

Computer and network security is increasingly becoming not only more significant to industry players but also complex regarding mitigating sophisticated cyber-attacks. It is essential for developers, systems administrators, and web administrators to develop and manage systems that can stand the test of time as far as computer and network attacks are concerned. A hybrid honeypot was deployed in the network setup of the Ghana Education Service. The honeypot setup was made up of Valhalla honeypot and honeyd (low-interaction honeypots), Cowrie (medium-interaction honeypot), Windows and two Ubuntu OS implemented on real systems (high-interaction honeypot) and Snort. This research goes a step further to collect the attack on data and analyse them. The attacks that were launched against the honeypots deployed in the network were Port Scanning, SSH Brute Force attack, HTTP Authentication Brute Force attack, SQL Injection and Spam. It was discovered that the honeypots received 5061 attack connections from October to December 2017. Majority of the attack connections were TCP based, resulting in 2851 of the total attack connections. The results of this work also show that honeyd receive 36% of the total attacks launched against the honeypots.
References


Index Terms

Computer Science  Security
Keywords