ABSTRACT

In digital era, the vulnerability of system is the main point to prevent attacks such as Port Scanning, Bruteforce and DoS that can make the system controlled by foreign parties and even paralyzed. So, solution for this problem is needed. Honeypot is security system to monitor and analyze every attack activity that enters the system. The selected honeypot types are low interaction honeypot (Dionaea) and medium interaction honeypot (cowrie) to secure the server. Different interactions allow both of them to have different abilities. The attacks chosen are Port Scanning, Bruteforce SSH and DoS with 2 scenarios, namely without honeypot and with honeypot. The results showed that Dionaea could catch more attacks than Cowrie. Meanwhile, in terms of interaction, Cowrie is superior. The QoS results of DoS attacks, before the honeypot was installed were throughput with indeks 4 categorized as very good, packet loss with indeks 4 being categorized as very good, delay with indeks 4 being categorized as very good, and jitter with indeks 2 being categorized as moderate. Meanwhile, after honeypot was installed, the throughput indeks was 4 categorized as very good, packet loss with indeks 4 is categorized as very good, delay with indeks 4 is categorized as very good and jitter with indeks 3 is categorized as good. Meanwhile, CPU usage rose 6.66% to 49% and Memory increased 12.48% to 37.6%.

Keywords: Honeypot, Cowrie, Dionaea, CPU, QoS