Annual conference of the South African Institute of Computer Scientists and Information Technologists (SAICSIT 2018), Port Elizabeth, 26-28 September 2018, pp. 164-170

Using network flow data to analyse distributed reflection denial of service (DRDoS) attacks, as observed on the South African national research and education network (SANReN): A postmortem analysis of the memcached attack on the SANReN

Burke, Ivan D
Herbert A
Mooi, Roderick D

ABSTRACT:

Distributed Denial of Service (DDoS) attacks cause significant disruption on critical networks within South Africa. Timely detection and mitigation is a key concern for the SANReN Cyber Security Incident Response Team (CSIRT). This paper presents an analysis on the Memcached reflection DDoS attack which occurred in February 2018. The attack was the largest DDoS attack to date. By analysing the attack and the impact it had on the SANReN network, this paper aims to show how network flow data can be used to detect network attacks, and perform post attack analysis to prevent future network attacks. The attack time-line is divided into three main phases: pre-attack, peek attack period and post attack residue.