Communications in Computer and Information Science

Utilisation of a virtual honeynet to proactively secure the South African National Research and Education Network against cyberattacks

Meyer, Heloise
Council for Scientific and Industrial Research (CSIR)
Meiring Naude Drive, Pretoria, 0184
Email: HPieterse@csir.co.za

South Africa is witnessing a significant increase in cyberattacks. Although such an increase in cyberattacks can be attributed to various factors, poor investment in cybersecurity technology and lack of awareness are causing South Africa to be a target of interest. While cyberattacks are targeting various sectors, it is the cyberattacks impacting critical infrastructure that are a growing concern. The South African National Research and Education Network (SA NREN) is a high-speed network dedicated to science, research, education and innovation traffic. With the growth of the SA NREN and the continuous increase in cyberattacks affecting South African institutions, proactive steps are required to secure and protect the SA NREN. This responsibility lies with the SA NREN Cybersecurity Incident Response Team (CSIRT), which was established in 2016 to offer protection against cyberattacks. While various proactive measures are currently in place to monitor the SA NREN, the CSIRT continues to explore alternative cost-effective solutions to secure the NREN. This paper investigates the benefits of utilising a novel low-interaction secure shell (SSH) honeynet, referred to as the Virtual Honeynet, to monitor and proactively secure the SA NREN. The Virtual Honeynet uses virtual containers to reduce resource requirements and improve performance. The investigation involved the experimental deployment of the Virtual Honeynet on the SA NREN over a twelve-day period and the evaluation of the captured data. The evaluation conducted focused on extracting behavioural and geographical intelligence from the raw data to guide the deployment of cyber measures to secure the SA NREN. The results presented in this paper confirm the value the Virtual Honeynet offers to the SA NREN as a technology to proactively secure the network.