Cray EX40 (Chicoma) Cluster Intrusion Detection Project

Abstract

Daniel Wild
Mentors: Skip McGee and Thomas Areba

LA-UR-23-28605

Security changes or configurations can often reduce the performance of a supercomputer or cluster (Shah, 2023). Analysis of a cluster's external network traffic provides an opportunity to identify potential malicious traffic, cluster misuse, or configuration problems without causing a negative performance impact. Using a mirror port, this project captured the external network traffic to and from the Cray EX40 (Chicoma) cluster for three months and analyzed it using two open-source intrusion detection tools, Suricata (Suricata, n.d.) and Zeek (Zeek, 2020). These intrusion detection tools were compiled and installed from source. Ansible roles and installation scripts were developed to automate future deployment and maintenance on production systems. The tools were tuned for high performance computing requirements using eBPF filters integrated in the build to bypass elephant flows and reduce packet loss. This project successfully identified security concerns such as excessive (approximately 1610) Secure Socket Shell connection attempts over a short (approximately 12 hour) time interval from a single source as well as four invalid certificates.

This project also identified several cluster configuration issues including anomalous switch and node Domain Name Service (DNS) queries, outbound Hypertext Transfer Protocol traffic with Automatic Private Internet Protocol Addressing and Transmission Control Protocol errors across the network. Anomalous node DNS queries were so prevalent that they encompassed approximately 97% of all DNS traffic within the network. Intrusion detection tools monitoring external cluster network traffic can provide security while enabling insights into configuration issues that can potentially increase cluster performance and improve the user experience.

References:

Shah, A. (2023, January 20). *Top HPC Players Creating New Security Architecture Amid Neglect*. Retrieved from HPC wire: h@ps://www.hpcwire.com/2023/01/20/top-hpc-players-creating-new-security-architecture-amid-neglect/

Suricata. (n.d.). Retrieved from Open InformaHon Security FoundaHon (OISF): h@ps://suricata.io

Zeek. (2020). Retrieved from The Zeek Project: h@ps://zeek.org/

Los Alamos NATIONAL LABORATORY