**Intrusion Detection System & Intrusion Prevention System: Suricata**

Originally, the IPS was going to be Wazuh, but with issues being heavily present in operating that program resulted in the switch to another open source software service called Suricata. Suricata was easily installed through the command line interface of the Linux virtual machine that was installed. Based on Suricata website, “Suricata is both an IPS and an IDS. It is mainly utilized for network level analysis and detection, but can also be utilized on a host level IDS or IPS.” (n.d. Suricata). The purpose of an intrusion detection system (IDS) is similar to that of an IPS. The only major difference between an IDS and that of an IPS is that an IPS will prevent unauthorized behaviors form occurring, outgoing and incoming. An IDS will detect and logs the suspicious behavior. It would be much more accurate to describe Suricata as a tool that logs data, but this data is malleable to the user to be utilized in conjunction with personal custom tools or to be used with more professional SIEMs.

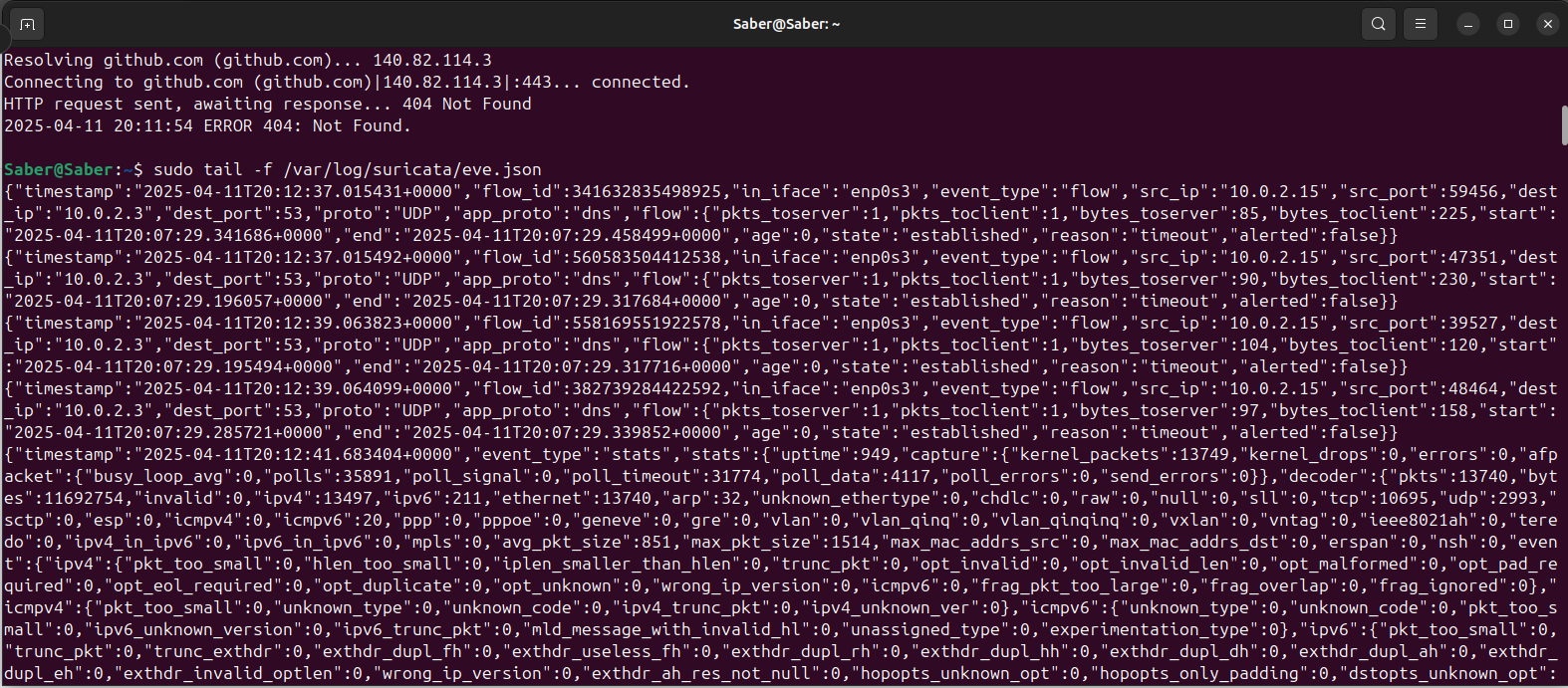
****

Figure 6: A screen capture of Suricata command line logging information.

Works Cited

Rodriguez, A. (2024). Small office Home Office Network Proposal [Unpublished manuscript]. Campbell University.

BlackHorse Solutions. (2023). AD2 Student Handbook [Unpublished instructional document].

“This document was acquired while doing an internship at BlackHorse solutions. This document provides a quick review of open source intelligence (OSINT) methodology along with security settings for various recommended browsers.”

(n.d.). *Suricata*. Suricata. <https://suricata.io/>

(n.d.). *Tenable Nessus® Essentials*. Tenable. https://www.tenable.com/products/nessus/nessus-essentials

(n.d.). *Entity relationship*. Lucidspark. https://lucidspark.com/