Desmond Hughes

Purdue University Global

IT262 Certified Ethical Hacking I

Cheryl Waters

September 10, 2022

Graphical user interface, text

Description automatically generated

Graphical user interface, website

Description automatically generated

Graphical user interface, application

Description automatically generated

Text

Description automatically generated

Graphical user interface, text

Description automatically generated

Graphical user interface, text

Description automatically generated

Graphical user interface, table

Description automatically generated with medium confidence

Part 2: Snort Alert is anomalous network and suspicious activity is reported. There are seven Snort Alert modes, which are Fast, Full, Console, Cmg, Unsock, Syslog, and None. Snort Alert analyses traffic with IP addresses when they pass through it, and are able to detect things like worms, port scan and other exploits. With Snort being an open source, it is easy to review the code. It catches security issues people may not have known about and saves time configuring firewalls, and to help with processing firewalls scan traffic.

There are some disadvantages that can cause Snort to not be affective, like when it comes to upgrading it, they can be hazardous, and also with updates it can get behind on them, which can sometimes be unstable. Snort can miss attacks due to low signal, because of a bad rule and because of the attacks it will not update properly. A feature that gives it a disadvantage is “Due to the extensive interface, it can be quite overwhelming to try and manage the product. There are many different places to go to set up individual items” (Israelsson, Karlsson & Giamarchi, 2005) With there being multiple places to go to set up the interface items it creates more of a problem by the interface is not simplified down and making it, so Snort has to cover more data. Snort also only looks for things in its ruleset, and because of this can not tell what traffic is considered to be normal from each host and it also can not tell what traffic is out of place, and will not be noticed unless it is setup to do so.

References

Israelsson, P., Karlsson, J., & Giamarchi, G. (2005). A quick overview of Snort. Retrieved 13 September 2022, from https://www.it.uu.se/edu/course/homepage/sakdat/ht05/assignments/pm/programme/Introduction\_to\_snort.pdf

Snort. (2022). Retrieved 13 September 2022, from <https://www.trustradius.com/products/cisco-snort/reviews>