Chad Ballay

**Week 6**

SNORT <https://www.snort.org/>

SNORT is an open source intrusion detection system(IDS) and intrusion prevention system(IPS). Cisco is the current maintainer and active developer. It is released under the GPL V2 and shows regular commits to it’s source code repo which point to an active and healthy community engagement. (<https://github.com/snort3/snort3>) This community engagement is key due to the need for continually having to update the rulesets for new attack patterns.

According to the snort web site, “It can perform protocol analysis, content searching/matching, and can be used to detect a variety of attacks and probes, such as buffer overflow, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more” (Snort FAQ, n.d.). So from a features perspective it fits the needs of business environment.

Part of the selling point for Snort is how lightweight it is. The practical advice is that if your hardware can run an OS that can run Snort then you can run Snort. This is how lightweight it is for both as Remote Sensor, Management Server, or a Monitoring Machine. So, in lean budget organizations this can be run with no additional hardware outlay beyond commodity servers. But this lightweight footprint does not imply lack of power.

SANS provides several whitepapers detailing various uses of Snort

<https://www.sans.org/reading-room/whitepapers/detection/detecting-torrents-snort-33144>

<https://www.sans.org/reading-room/whitepapers/detection/snort-distributed-intrusion-detection-system-352>

<https://www.sans.org/reading-room/whitepapers/detection/build-leverage-snort-ids-metrics-reduce-risk-34350>

There are also several other guides I found for creating a Snort testlab that could be used to build a production ready installation.

<https://medium.com/@Alibaba_Cloud/how-secure-your-linux-server-using-snort-nids-6fc04dd1b35d>

<https://www.techrepublic.com/article/using-snort-for-intrusion-detection/>

Snort fills the niche for smaller businesses that need and IDS/IPS solution and are willing to trust the wisdom of the crowd. It is time tested and flexible enough to fit their needs while it’s broad adoption and lengthy history means finding vendors willing to support a Snort install should be easy.