Hackfest November 2014

News

http://www.digitalcommunities.com/articles/DARPA-Director-Calls-for-Cybersecurity-Change.html

Drupal 7 Database Exploit:
https://www.drupal.org/SA-CORE-2014-005

Suricata

Multi-theaded

IDS vs IPS
Log network or block attacks

Barnyard - log data to disk or database (increase performance)

libhtp - log HTTP [Do not use in Production (??)] = log requests, log certificates, block executables

NO TLS/SSL proxy = probably going to be a security alert and handled in the browser soon anyway - Example Chrome

IP Reputation: Good hosts, bad hosts, and shared hosting machines - Block botnets or spam

Snorby GUI

http://www.linux.org/threads/suricata-the-snort-replacer-part-1-intro-install.4346/

http://hackertarget.com/install-suricata-ubuntu-5-minutes/

https://redmine.openinfosecfoundation.org/projects/suricata/wiki/CentOS_64_Installation_(with_unix_socket_geoip_profiling_and_MD5_features)

http://blog.inliniac.net/2014/03/30/video-suricata-2-0-installation-and-quick-setup/

http://cyruslab.net/2012/10/18/building-an-ids-part-1-installing-pre-requisites-and-snorby/

http://blog.securityonion.net/p/securityonion.html