Network intrusion detection with open source

Suricata

Official page: https://suricata.io/

Rules syntaxis: https://suricata.readthedocs.io/en/suricata-6.0.0/rules/intro.html

Free Suricata rules libraries:

https://rules.emergingthreats.net/open/
https://openinfosecfoundation.org/rules/trafficid/trafficid.rules
https://raw.githubusercontent.com/ptresearch/AttackDetection/master/pt.rules.tar.gz
https://sslbl.abuse.ch/blacklist/sslblacklist.rules
https://sslbl.abuse.ch/blacklist/ja3_fingerprints.rules
https://security.etnetera.cz/feeds/etn_aggressive.rules
https://raw.githubusercontent.com/travisbgreen/hunting-rules/master/hunting.rules
https://malsilo.gitlab.io/feeds/dumps/malsilo.rules.tar.gz

Snort

Official page: https://www.snort.org/snort3

Infographic: https://www.snort.org/documents/snort-rule-infographic

Security Linux distributions

SELKS: https://www.stamus-networks.com/selks

pfSense: https://www.pfsense.org/

SecurityOnion: https://securityonionsolutions.com/software

Info

Network TAP: https://www.gigamon.com/resources/resource-library/white-paper/understanding-network-taps-first-step-to-visibility.html

How to build Network TAP: https://www.youtube.com/watch?v=2tsvBnTIjFo

Zeek for network behavior analytics: https://www.youtube.com/watch?v=NZytrNOUzzE

tcpdump basics – CLI packet capture: https://www.howtouselinux.com/post/tcpdump-cheat-sheet

Extra free tools: https://www.activecountermeasures.com/free-tools/

Metaspoitable - test machine with tons of vulnerabilities: https://information.rapid7.com/download-metasploitable-2017.html

OpenVAS a.k.a. GreenBone – vulnerability assessment tool to make some noise: https://www.greenbone.net/en/testnow/#toggle-id-3

Scapy - packet crafting tool: https://scapy.readthedocs.io/en/latest/usage.html