ids2

Installing from VA
https://www.prelude-siem.org/projects/prelude/wiki/InstallingVA

The Zeek Network Security Monitor
https://www.zeek.org/

What is Bro IDS [Zeek]? And Why IDS Doesn't Effectively Describe It [Overview and Resources]
https://bricata.com/blog/what-is-bro-ids/

Snort
https://www.snort.org/

MONITOR THE SAFETY OF YOUR INFORMATION SYSTEM
https://www.prelude-siem.com/en/prelude-siem-en/

What's new in Prelude NG
https://www.prelude-siem.com/en/whats-new-in-prelude-ng/

Intrusion Detection: Snort, Base, MySQL, and Apache2 On Ubuntu 7.10 (Gutsy Gibbon) (Updated)
https://www.howtoforge.com/intrusion-detection-with-snort-mysql-apache2-on-ubuntu-7.10-updated

ids

Network intrusion detection system
https://patents.google.com/patent/US20100251370A1/en

Using decoys by a data loss prevention system to protect against unscripted activity
https://patents.google.com/patent/US8549643B1/en

things to assist in packet analysis
https://github.com/noahdavids/packet-analysis/blob/master/README.md

Taxonomy and Survey of Collaborative Intrusion Detection
https://dl.acm.org/doi/10.1145/2716260

Snort 2 DCE/RPC Preprocessor Buffer Overflow
https://www.rapid7.com/db/modules/exploit/multi/ids/snort_dce_rpc

community rules

Snort Rule for the Bluekeep Module in Metasploit
https://medium.com/@alexandrevvo/snort-rule-for-the-bluekeep-module-in-metasploit-17613066915d

span / port-mirror

RSPAN and 2950 switches
https://community.cisco.com/t5/other-network-architecture/rspan-and-2950-switches/td-p/353667

Configuring Local SPAN, RSPAN, and ERSPAN
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/span.pdf

Configuring SPAN and RSPAN
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_40_se/configuration/guide/scg/swspan.pdf

Understanding SPAN,RSPAN,and ERSPAN
https://community.cisco.com/t5/networking-documents/understanding-span-rspan-and-erspan/ta-p/3144951

Configuring Local SPAN, RSPAN, and ERSPAN
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/span.pdf