

Teil II

Verfügbare Open-Source- Intrusion-Detection- Systeme



In diesem Teil werden die wesentlichen Open-Source-Lösungen vorgestellt.

1. Selfmade IDS

- Verwendung allgemeiner Dienste
- find/diff
- tcpdump/ngrep

2. Hostbasierte IDS
 - Automatische Protokollanalyse
 - Tripwire
 - Linux-Intrusion-Detection-System – Lids
 - System iNtrusion Analysis and Reporting Environment – SNARE
3. netzwerkbasierte IDS
 - snort