

**Table 1 – OSSIM Security Tools**

<b>Application</b>	<b>Purpose</b>
Arpwatch	Used for MAC anomaly detection
P0f	Used for passive OS detection and change analysis
Pads	Detects service anomalies
Nessus	Vulnerability assessments, scanner
Snort	Open- source network intrusion detection system (IDS)
Spade	Statistical packet anomaly-detection engine for use against attacks that don't currently have signatures (e.g., those in Snort)
Tcptrack	Tracks session data information, which can grant useful information for attack correlation
Ntop	Tracks network information over time for networks and hosts
Nagios	Monitors host and service availability information
Osiris	Host IDS
OCS-NG	Cross-platform inventory solution
OSSEC	Integrity, rootkit, and registry detection