**Tampering with SysLog**

**Note: We could not find any definition for Tampering with SysLog. We present our definition of Tampering with syslog.**

**Description**

Computer system designers may use syslog for system management and security auditing as well as general informational, analysis, and debugging messages. A wide variety of devices, such as printers, routers, and message receivers across many platforms use the syslog standard. This permits the consolidation of logging data from different types of systems in a central repository. Implementations of syslog exist for many operating systems. (definition of syslog from wikipedia) An attacker can target syslog (who is usually an insider) removes syslog, allowing him to **remove evidences** of a malicious activity. As a result, removed log files might lead to a **failure in accountability**, **non-repudiation** and **incident forensics capability**. ( specific form of log removal)