Identifying attacks

The remaining group of systems whose logfiles are likely to be of interest is servers. Whilst logs from clients and intermediaries will usually indicate attacks against other sites, logs from servers will normally be used to detect attacks, or attempted attacks, either on the servers themselves or on other local systems. Public servers such as web or mail systems are likely to be the most exposed to hostile activity on the Internet so these should always be configured to keep good and secure logs. Internal servers should also record logs as these may be subject to attack from within the organisation, or may be used by malicious local users to practice before attacking systems elsewhere. Detecting and preventing such activity at an early stage by recording and monitoring server logs can save the organisation a great deal of trouble.

Attacks against servers generally have one of two intentions. One is to gain access, presumably unauthorised, to the information or services supplied by that particular server; students might well be motivated to try to gain access to the server that contains their examination results, for example. The second aim is to make a server perform some function for which it is not intended, for example to make it act as an intermediary in another attack, as shown in Section 4.4. Traces of these two types of attack will often appear in different sets of logfiles. It is therefore essential to ensure that both types of logs are recorded and checked regularly for suspicious activity. All logs should record both successful and unsuccessful attempts to use the system. Repeated failures to log in may indicate an attack, a configuration problem or a user problem.

Authentication Logs

Systems that require authentication should always keep a record of the users who authenticated successfully, and also of failed attempts to authenticate. Where a number of consecutive failures cause an account to be locked out, this must be recorded. In most cases the system should take additional measures to alert the operator to this event. Authentication failures may be due to mishaps – genuine users can mistype or forget their passwords – but any patterns of failures should be investigated. Authentication logs should also be checked for any unexpected periods of silence, as these may indicate that an intruder has been able to tamper with the logs to conceal evidence of their activities. Entries in authentication logs should always be associated with an accurate time; where a single authentication gives access to a session, rather than a single transaction, it can also be helpful to record the time when the session ended. 5.2 Service Logs

Servers that are accessible to untrusted users should also retain logs of the requests made to them. For example, public web servers should usually record the URLs requested by their clients. The time and the IP address from which the request came should also be retained. As with authentication logs, unusual events are often a sign of problems. These may include periods of unusually low or high activity, though web servers in particular can see unexpected surges in legitimate requests. A common way to attack a server is to present it with

unexpected input: very long requests, or those containing unusual characters, should be investigated, as should any request containing the name of a command interpreter, such as **/bin/csh** or **cmd.**exe. Service logs often cannot show whether an attack was successful – even a request that failed as far as the service is concerned may have achieved its malicious purpose before it was rejected.

Summary of Logs

Type of System	**Logs required**
Authentication service	• userid + time + login success/fail + sc (userid + time + logout) details of lock
Information service	• source IP + time + request + result

Source URL: https://community-stg.jisc.ac.uk/library/janet-services-documentation/identifying-attacks