Authentication Log Reviewer: Design Document

Authors

- Alex Clark (ayc55)
- Reuben Rappaport (rbr76)

Criteria for Intrusion

1. The first case qualifying as intrusion which we chose was multiple failed attempts to ssh into the system by a single user within a short time interval, i.e. >3 failed attempts within a 1-minute period.
2. The second case qualifying as intrusion was a sufficiently large number of ssh attempts within a 1-minute period, beyond the number of users which would be expected for the system. Specifically, a case where >150 failed ssh attempts across all users occurred within a 1-minute interval would be flagged as a possible intrusion.

Justifications for Criteria

1. This was chosen due to 3 seeming to be a reasonable threshold for the number of failed authentication attempts a legitimate user might encounter, under circumstances like mistyping or forgetting one's password. Beyond this point, it is more likely that the detected behavior would be an instance of a malicious user attempting to guess another's credentials.
2. This was chosen due to our estimates of the expected workload for the system. A server with approximately 100 users, all of whom login at least once per day, can reasonably be expected to have most users succeed at their login attempts. Even if all users needed to access the server at the same time, generously assuming an average of one failed login per user, this should not result in a number appreciably greater than 100 failed attempts within a single minute.

Potential False Positives

One false positive, which is not outside the bounds of possibility, would be a user legitimately experiencing greater than 3 failed login attempts. Situations which could cause this might involve having forgotten one's password, or having issues typing it correctly due to factors like an unfamiliar device, sleep deprivation, or drunkenness. This could be investigated rather easily upon review of the syslog file, however, and determining whether the user exhibited other suspicious behavior after logging in.

Another potential false positive would be an event where due to server issues, many users were experiencing failed login attempts and repeatedly attempting to connect to the server, e.g. when attempting to submit an assignment close to the due date. This could again be recognized as expected behavior upon review.

Potential False Negatives

A potential false negative would be a malicious user correctly authenticating with credentials they are not authorized to use. In the event they had stolen another user's password, it would be reasonable for them to succeed at this without failed authentication attempts.