Megan Massie, Connor Calabria
Dr. Ong
AC 314.01
25 April 2025

LOGIN FORENSICS: CYBERSECURITY CASE ANALYSIS

Part 1

C. Based on the data, the total number of login attempts made on each day of the week is as follows: Monday had 235,521 logins, Tuesday had the most with 252,117, followed by Wednesday with 249,695. Thursday and Friday were slightly lower at 232,287 and 240,374, respectively. Logins dropped a lot on the weekend, with Saturday only having 59,952 and Sunday the least at 22,234.

This distribution of logins makes sense for a company that most likely runs on a standard Monday-to-Friday schedule. It's normal to see higher login activity during the weekdays, especially in the middle of the week (Tuesday through Thursday), when people are most likely to be working. The big drop in logins on Saturday and Sunday lines up with the expectation that the system is being used mostly during regular business hours, and any major spikes or logins outside of these patterns could be worth looking into more closely.

Part 2

B. Based on the data, there are some glaring issues based on the failure rate of employees. The Username, Admin, has a failure rate of 100%, which means that there could be an error with this account, or there is potential for fraud with this account. This should require immediate attention and should be highly monitored. Also, there are several accounts that have high failure rates, such as Evyn Jeanneau who has a failure rate of 81.98%. These are users who are employees in the employee log, so these accounts with high failure rates should be tracked to see if these login attempts were made after the employees were possibly terminated, or if these accounts were hacked. For example, Evyn Jeanneau had significantly more login attempts than other accounts, indicating that her account may have been hacked. With these high failure rates, these accounts should be investigated in order to ensure there are no problems within these user accounts.

C. Based on the volume of attempts, it should be recommended that the company has a system that automatically terminates employee accounts once they are fired and gets rid of all of their controls. On top of this, more audits of these files and attempts made by terminated employees should be conducted to ensure that no potential damage is caused to the company. Also, former employees with a high volume of attempts should be flagged, and further investigation should be made into these accounts.

E. The only username on the log file that is not contained within the employee log file is the Admin username. Not only was this the only account, but this account only has made unsuccessful login attempts. 1043 login total attempts were made. This could be a decoy account designed to try and gain unauthorized access, or there may in fact be a legitimate error with the administration account. Either way, as this account name represents an important level of employee within the company and as only unsuccessful attempts were made, this account should be investigated in order to ensure there is no threat of attack from this account.

Part 3

Based on the data, we found suspicious users by looking at employees who were still active and had logged in before, but didn't have any logins on the dates when login records were missing. We defined active employees as those who had an existing history of login attempts and had no end date listed in their employee file. After running this analysis, we narrowed it down to one main user: Dsketch, who we found out is David Sketch in the employee records. Since David Sketch had logged in normally before but had no logins at all during the suspicious dates, it's likely he could have been involved with deleting or tampering with the login records. The fact that he was active before but completely silent during the missing entries makes him stand out and should definitely be looked into more.

At the same time, there are other employees that could also have had reasons to delete records. From earlier parts of the project, we found people like Kameko Mathwen, who kept trying to log in even after they were terminated in 2014, which could be suspicious too. There were also users with really high failure rates, like Evyn Jeanneau who failed 81.98% of their login attempts, which might suggest an incentive to cover up additional failed attempts through the deletion of login records.

Part 4

This section analyzes login activity on four U.S. holidays when the company was officially closed in the year 2022: Memorial Day (May 30), Independence Day (July 4), Labor Day (September 5), and Thanksgiving Day (November 24). Our goal was to determine whether login behavior on these dates aligned with expectations by comparing different data points from the listed holidays to year-round daily averages. We focused on five areas: 1) overall login volume, 2) geographic location of logins, 3) number of unauthorized attempts, 4) distinct IP addresses used, and 5) the volume of activity during off-hours (6PM to 6AM). Through this investigation, we hope to uncover any potential issues related to access controls.

Across most holidays, login activity was low and consistent with the expectation that fewer employees would access the system. Memorial Day saw 164 login attempts, Labor Day 169, and Thanksgiving 180. These numbers are all well below the company's daily average of approximately 3,540 login attempts. However, Independence Day was a clear outlier. That day alone saw 8,533 login attempts, which is more than twice the daily average.

This spike led us to look at where the logins were coming from. Illinois, the company's most common login location year-round, was still the most common during the holidays. However, on Independence Day, 8,444 of the login attempts originated from Pyongyang, North Korea. This city does not appear in non-holiday login activity and is not tied to the company's known operations. That volume of access from a location that otherwise does not show up in the data is difficult to explain as legitimate use.

We also reviewed the time of day when these logins occurred. On typical days, around 373 logins occur between 6PM and 6AM. During most holidays, this number was even lower (27 for Memorial Day, and 17 for both Labor Day and Thanksgiving). On Independence Day, however, there were 6,551 logins during off-hours. This suggests that a large portion of the activity occurred when system monitoring might be less active.

We then looked at distinct IP addresses per user. Most holidays showed just one IP, indicating consistent and expected usage. On Independence Day, that number rose to 2.36. This level of variability in network origin further separates this holiday from the others. It is unlikely that a single user would legitimately log in from more than two IPs in one day.

Finally, we considered the volume of unauthorized login attempts. Memorial Day showed only two, and the year-round average for non-holidays was around five per day. While we did not detect a large number of unauthorized attempts on Independence Day directly, the volume and pattern of activity raise the possibility that some were hidden within the broader surge.

Taken together, these findings point out that Independence Day does not follow the pattern of the other holidays and data from this day is inconsistent with regular employee behavior. The combination of high volume, unfamiliar location, off-hour activity, and unusual IP variation suggests that there was an intentional attempt to access the system on July 4th 2022. While we cannot say for certain what caused this spike, the data points to a potential access control weakness that could be exploited when oversight is reduced.