Joneslis1
300573902
ENGR123_Lab3

Q1:

Incorrect password count: 14482

Q2:

Failed username: 5857

Q3:

Success between march+april: 21

Q4:

Average success for each month (i added values of 0 for days not in entry):

- April = 2.7
- March = 1.032
- Across both: 1.866

Q5:

Failed logins:

- April = 20333
- May = 6

Q6

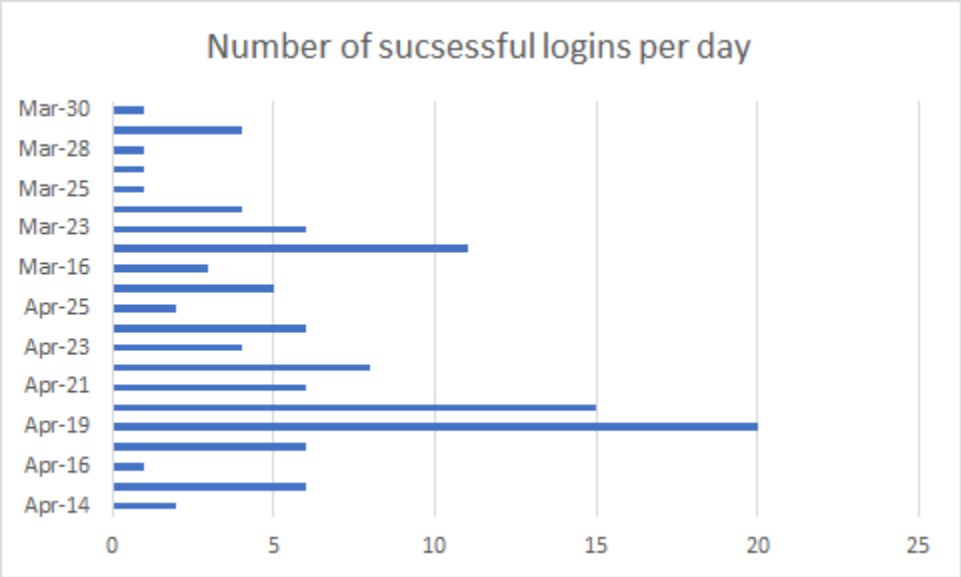
Average failed logins per month

- April = 677.77
- 0.19

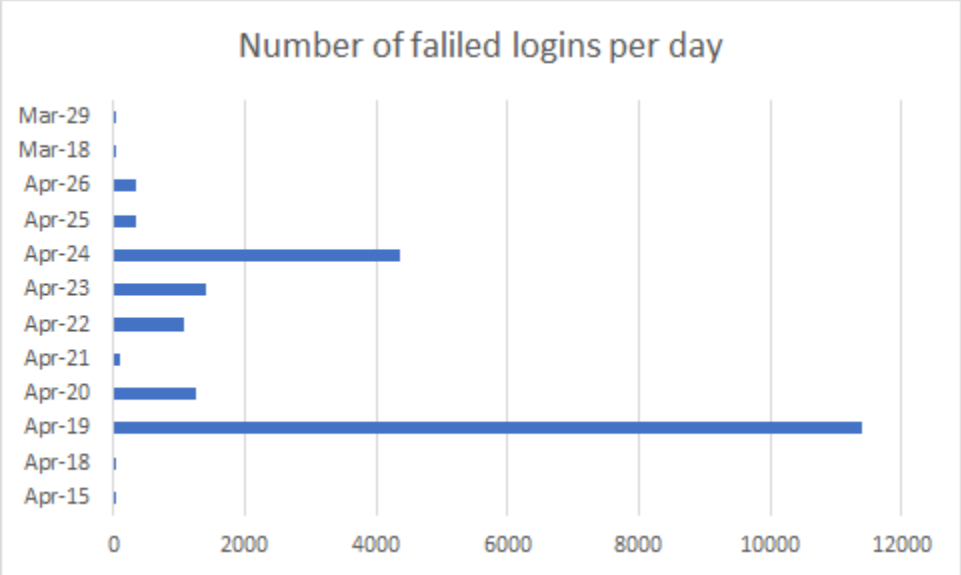
Q7:

The attacks would be a dictionary attack if there is a small difference in login attempts between each unsuccessful login on the same user. This can also mean a large amount of attacks within a small amount of time which is consistent for a lot of days in april

Q8:



Q9



Q10:

Top 5 usernames for failed:

1. Root
2. Admin
3. Test
4. Administrator
5. 123456

Q11:

Only real user is Root

Q12:

The top usernames that aren't actually users were probably selected based on the most common head roles (admin for the server / site and root). Based on the extremely large quantity of fails for root compared to the next top 4, my guess is that the attacker started the brute force attack on the other 4 and quickly turned it off after a few seconds of attacking.

Q13:

Top 3 failed IP addresses:

1. 219.150.161.20
2. 8.12.45.242
3. 222.66.204.246

Q14:

Address of top 3 failed IP networks

1. Address 1 = China - Henan
2. Address 2 = Germany - Frankfurt am Main
3. Address 3 = China - Shanghai

Most common region: China

Q15:

All compromised accounts:

- DHG - both logins are in the Dominican republic but different regions
- Root
- User1
- User3

Q16

- DHG - both logins are in the Dominican republic but different regions and 20 logins within the same region
- Every other account has multiple different countries logins so the likelihood of these accounts being compromised is high