ІПЗ-33\1 Гоша Давід Олександрович

Лабораторна №5

Тип атаки	Область перебору	Довжина паролю	Пароль	Час
За допомогою перебору	Всі друковані символи	від 1 до 4 символів	veg1	1.702 секунди
За допомогою перебору	Малі латинські і Всі цифри	від 1 до 4 символів	veg1	0.053 секунди
По словнику	Словник	-	bear	0.01 секунди
За допомогою перебору	Всі друковані символи	-	bear	0.728 секунди
За допомогою перебору	Малі латинські	-	bear	0.007 секунди

Висновки

Складність пароля в комп'ютерній промисловості зазвичай оцінюють у термінах інформаційної ентропії (поняття з теорії інформації), що вимірюється у бітах. Замість кількості спроб, які необхідно зробити для вгадування пароля, обчислюється логарифм на підставі 2 від цього числа, і отримане число називається кількістю бітів ентропії в паролі. Пароль з, скажімо, 42-бітною складністю, порахованою у такий спосіб, буде відповідати випадково згенерованому паролю завдовжки 42 біта. Іншими словами, щоб методом повного перебору знайти пароль із 42-бітною складністю, необхідно створити 242 паролів та спробувати використовувати їх; один із 242 паролів виявиться правильним. Згідно з формулою зі збільшенням довжини пароля на один біт кількість можливих паролів подвоїться, що зробить завдання атакуючого вдвічі складніше. У середньому

атакуючий повинен перевірити половину з усіх можливих паролів до того, як знайде правильний. Через парадокс днів народжень.

Як результат — не можна дати точну відповідь на деяку міру іншу проблему, проблему оптимальної складності пароля. Національний інститут стандартів та технологій (США) (NIST) рекомендує використовувати пароль з 80-бітною ентропією для найкращого захисту, який може бути досягнутий за допомогою 95-символьного алфавіту (тобто, набір символів з ASCII) 12-символьним паролем (12*6,5 біта = 78).

Тому мінімально надійний пароль повинен містити 12 символів, заголовну літеру, спец символ та цифру.

Якщо мі намагаємося підібрати такий пароль, нам знадобиться що найменше 2^{39} спроб для досягнення успіху з 80% шансом. Нам знадобиться $1,45 * 10^{29}$ хвилин. А це багато мільйонів століть.

Тест

1. В, Г
2. А, Б
3. А
4. А,Б,В
5. Б
6. В
7. В
8. А,Б
9. В
10. Г