ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ ПРОГРАММНЫХ СРЕДСТВ РАСШИФРОВКИ ПАРОЛЕЙ НА ОСНОВЕ АНАЛИЗА ХЭШЕЙ

Макатерчик А.В.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Маликов В.В. – канд. техн. наук

Использование хеш-функций находит широкое применение. В интересах защиты информации важно понимать и знать реальное состояние дел с уровнем возможностей используемых технологий. Данное исследование направлено на анализ возможностей программных средств анализа и расшифровки паролей, функционирующих на основе методов анализа хэшей.

Использование хеш-функций находит широкое применение в различных областях информационной безопасности. Целесообразность использования хеш-функции в криптографическом преобразовании документов при передаче сообщений в вычислительных сетях различнного назначения, в том числе и специального в настоящее время не вызывает сомнений. В современных системах электронного документооборота в ЛВС «среднего уровня» (до 10 тыс. абонентов) хеширование представляется необходимым встроенным средством для распределения и защиты информации абонентов сети [1].

Однако, техническая осведомленность злоумышленников и их инструментарий постоянно растут и изменяются, поэтому в интересах защиты информации является жизненно необходимым знать реальное состояние дел с уровнем возможностей используемых технологий защиты информации. Данное исследование направлено на анализ возможностей программных средств анализа и расшифровки паролей, функционирующих на основе методов анализа их хэшей.

Различные по своей природе утечки хэшей паролей и учетных записей являются в настоящее время распространѐнным явлением. Утилиты взлома паролей в своем функционировании опираются на следующую логику: Функция хэширования преобразует пароли во внешне хаотичный набор символов, которые теоретически не обратимы обратно в пароль. Однако одинаковые пароли, имеют одинаковый хэш в случае вычислении его с помощью одинаковой функции. Соответственно, при использовании таблицы зависимостей вероятных паролей и их хэшей от используемой функции, позволяет обнаруживать подходящий пароль [2].

На первом этапе исследования были выбраны для исследования следующие программные средства:

скрипт определения хэш-функции hash-identifier;

списки паролей RockYou;

программа расшифровывания Hashcat.

Hashcat позволяет проводить атаку по словарю, гибридную атаку, атаку по маске и атаку на основе правил.

Анализ проводился с использованием контрольных слов, входящих в список RockYou и не входящих в него. Кроме того, для контрольных слов из списка RockYou применяются различные комбинации регистров, фрагментов этих слов.

В исследовании использовался компьютер на основе процессора i5-6300hq. В данное утилите есть возможность производить вычисления на видеокартах, что значительно ускорило бы брут-форс.

После установки программных средств, выполнено хеширование контрольных слов с использованием следующих функций: MD5, SHA1, SHA256, SHA384, SHA512, gost, RIPEMD, MD4, SHA224, Whirlpool.

На первом этапе проверены возможности атаки прямым перебором. При брут-форсе в исследуемой программе есть возможность указать диапазон длин паролей, а если заранее известна какая-либо информация о пароле, то можно использовать брут-форс по маске, что ускорит его работу. На данном этапе применялись хэши простых цифровых паролей длинной от 3 до 10 символов.

В рамках исследования был создан файл с 3 хэшами sha512 для перебора с использованием маски суммарно на подбор всех паролей ушло 25 минут, скорость перебора около 5000-6000 тысяч хэшей/с.

Для полного перебора файла с 5 разными хэшами md5. Для перебора всех паролей длинной до 7 символов понадобилось менее 30 мин.

Для подбора одного пароля длинной 8 символов было потрачено около 2 минут при скорости 90000-100000 тысяч хэшей/с.

Для расшифровки 5 хэшей паролей длинной более 8 символов потребовалось 17 часов.

Расшифровка более сложных паролей методом прямого перебора оказалась на данном оборудовании была физически нереализуемой.

Расшифровка по словарю. Выполняется по отдельности для каждого контрольного слова.

Результаты исследования сведены в таблицу 1.

Таблица 1 – Результаты анализа возможностей программных средств расшифровки паролей.

№п/п	Определение хэш-функции hash-identifier	Расшифровка программой Hashcat
Слово из списка RockYou (латиница)	Верно	
Слово из списка RockYou (кириллица)	Верно	Ошибка
Слово из списка RockYou (латиница) с измененным регистром	Верно	Ошибка
Фрагмент слова из списка RockYou (латиница)	Верно	Верно
Слово не из списка RockYou (латиница)	Верно	
Слово не из списка RockYou (кириллица)	Верно	Ошибка
Слово не из списка RockYou (латиница) содержащее в себе слово из списка	Верно	Ошибка

Копии экранов с примерами работы исследуемых программ приведен на рисунке 1.

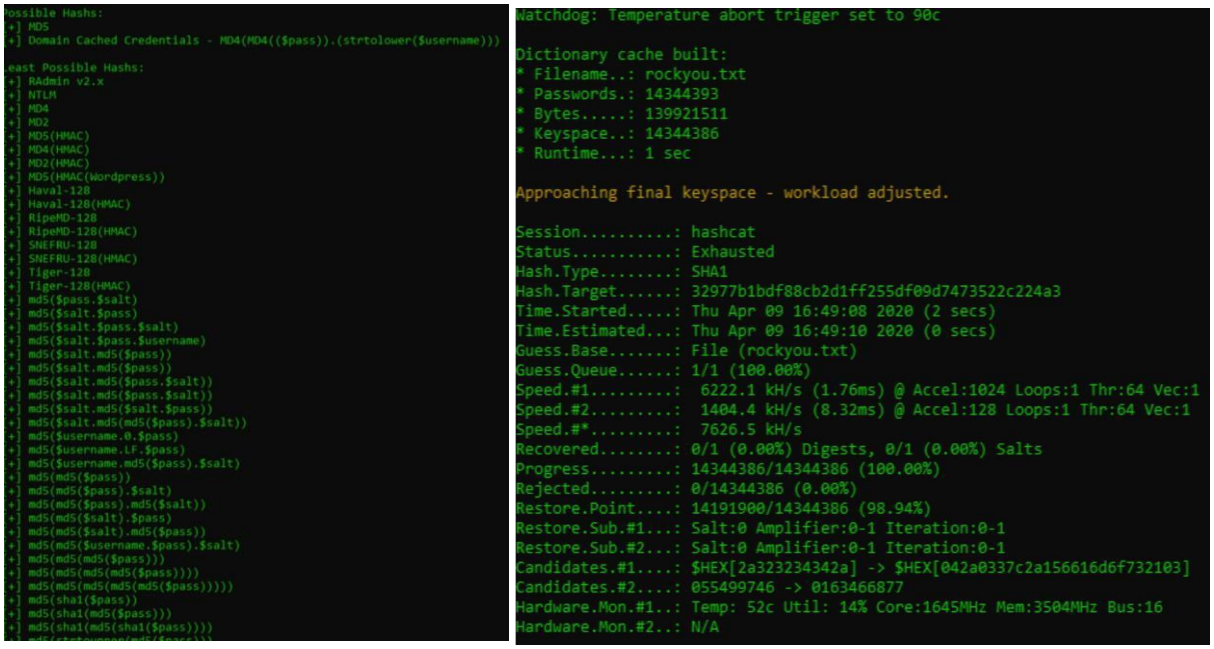

Рисунок 1 – Примеры функционирования исследуемых программ

Результаты исследования позволяют утверждать, что реальные возможности существующих программных средств по расшифровке паролей на основе анализа хэшей достаточно ограничены. При этом стоит учитывать, что идентификация хэш-функции выполняется быстро и достоверно, что значительно повышает эффективность расшифровки паролей. И можно утверждать, что способ хэширования на расшифровку не влияет.

Выявленные ограничения возможностей программных средств:

брут-форс сложных паролей практически невозможен;

обязательным условием расшифровки хэша, является нахождение захэшированной информация в словаре либо как целое слово, либо как часть другого слова;

поддерживается только латиница.

Список использованных источников:

1. Родионов Александр Сергеевич, Сухарев Сергей Леонидович Использование хеш-функции для защиты информации в локальных вычислительных сетях военного назначения // Известия ЮФУ. Технические науки. 2012. №5. URL: https://cyberleninka.ru/article/n/ispolzovanie-hesh-funktsii-dlya-zaschity-informatsii-v-lokalnyh-vychislitelnyh-setyah-voennogo-naznacheniya (дата обращения: 17.03.2020).

2. Kody. Определения типов хэшей при помощи скрипта hash-Identifier для расшифровки паролей [Электронный ресурс] / Kody // Электронный журнал Securitylab.ru. – 2020г. – Режим доступа: https://www.securitylab.ru/analytics/506412.php (дата обращения: 05.04.2019).

3. Иванов Михаил Александрович Способ обеспечения универсальной защиты информации, пересылаемой по каналу связи // Вопросы кибербезопасности. 2019. №3 (31). URL: https://cyberleninka.ru/article/n/sposob-obespecheniya-universalnoy-zaschity-informatsii-peresylaemoy-po-kanalu-svyazi (дата обращения: 17.03.2020).