тулзы для pwd cracking

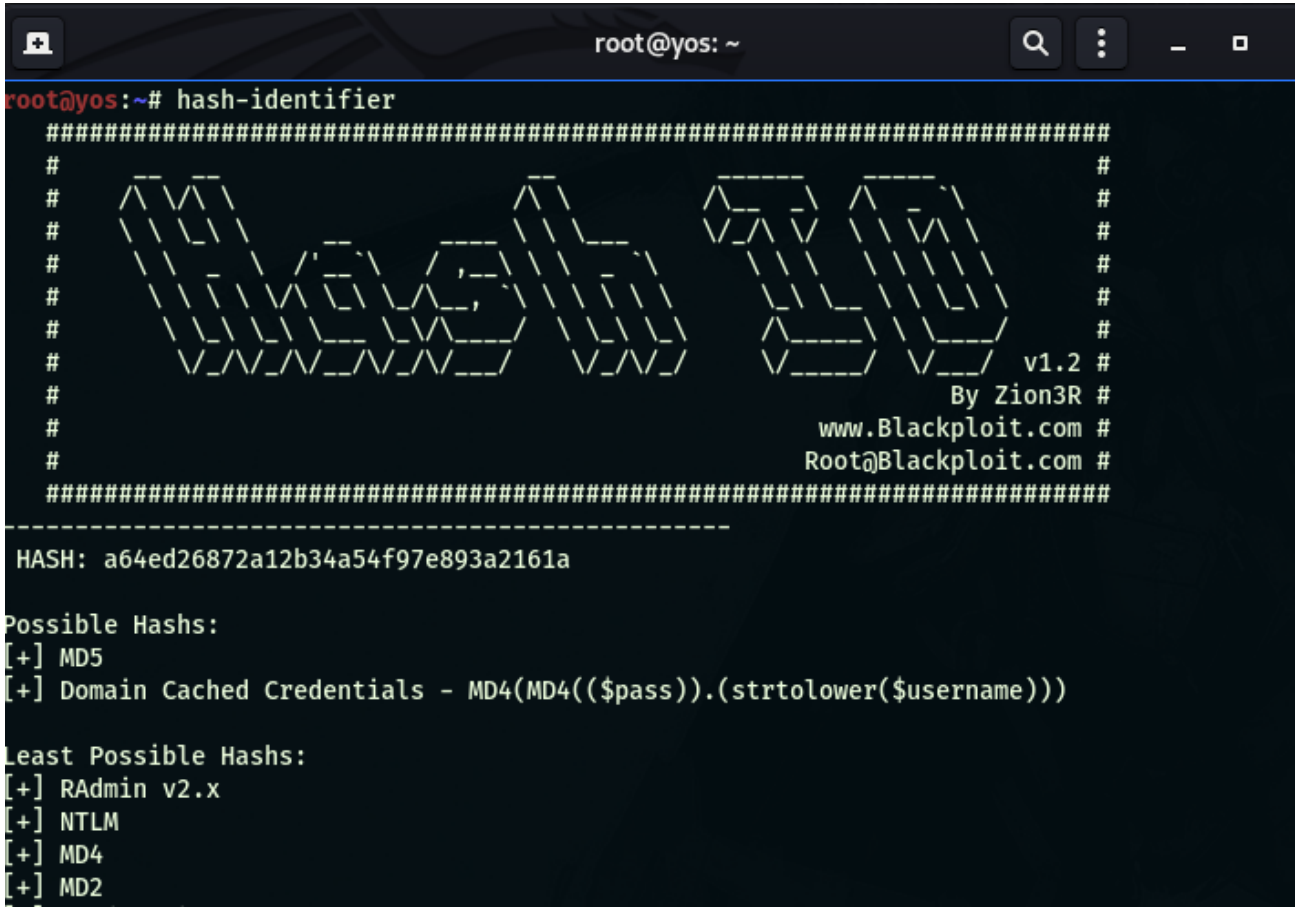
список основных инструментов для решения тасков

ОСНОВНЫЕ ПОНЯТИЯ

- хэш-функции — это функции, предназначенные для «сжатия» произвольного сообщения или набора данных, записанных, как правило, в двоичном алфавите, в некоторую битовую комбинацию фиксированной длины, называемую сверткой
- статья 272
- статья 137
- брут — метод взлома путем подбора паролей. суть подхода заключается в последовательном автоматизированном переборе всех возможных комбинаций символов с целью рано или поздно найти правильную.
- соль — строка данных, которая передаётся хеш-функции вместе с входным массивом данных для вычисления хэша

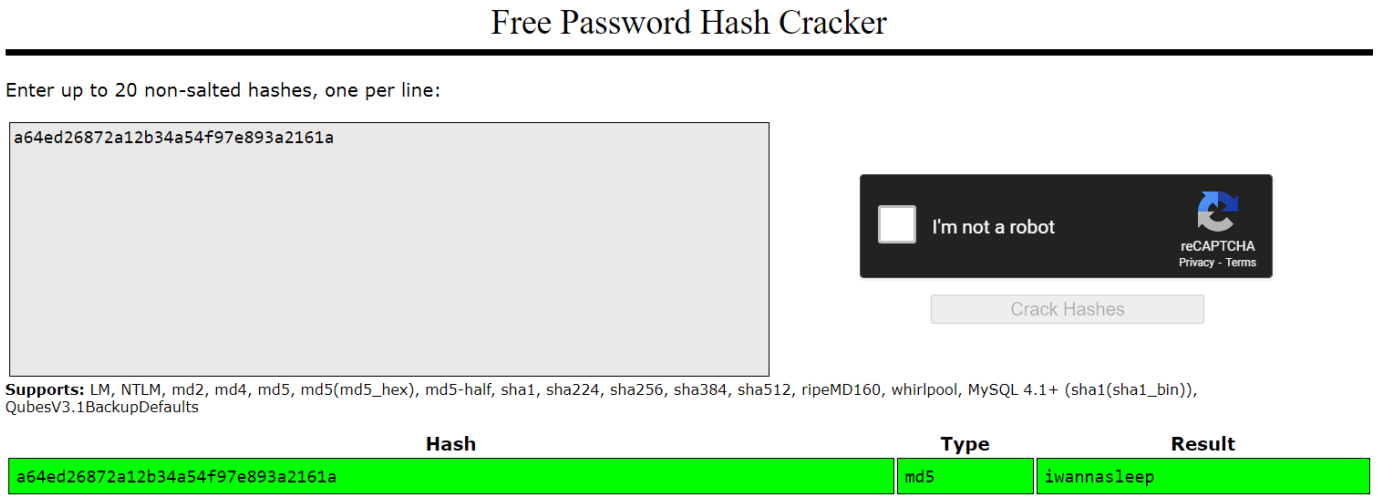
HMEX

> hash-identifier



скрипт hash-identifier позволяет определить тип любых хэшей, чтобы затем указать правильный режим при работе с Hashcat.

> crackstation.net



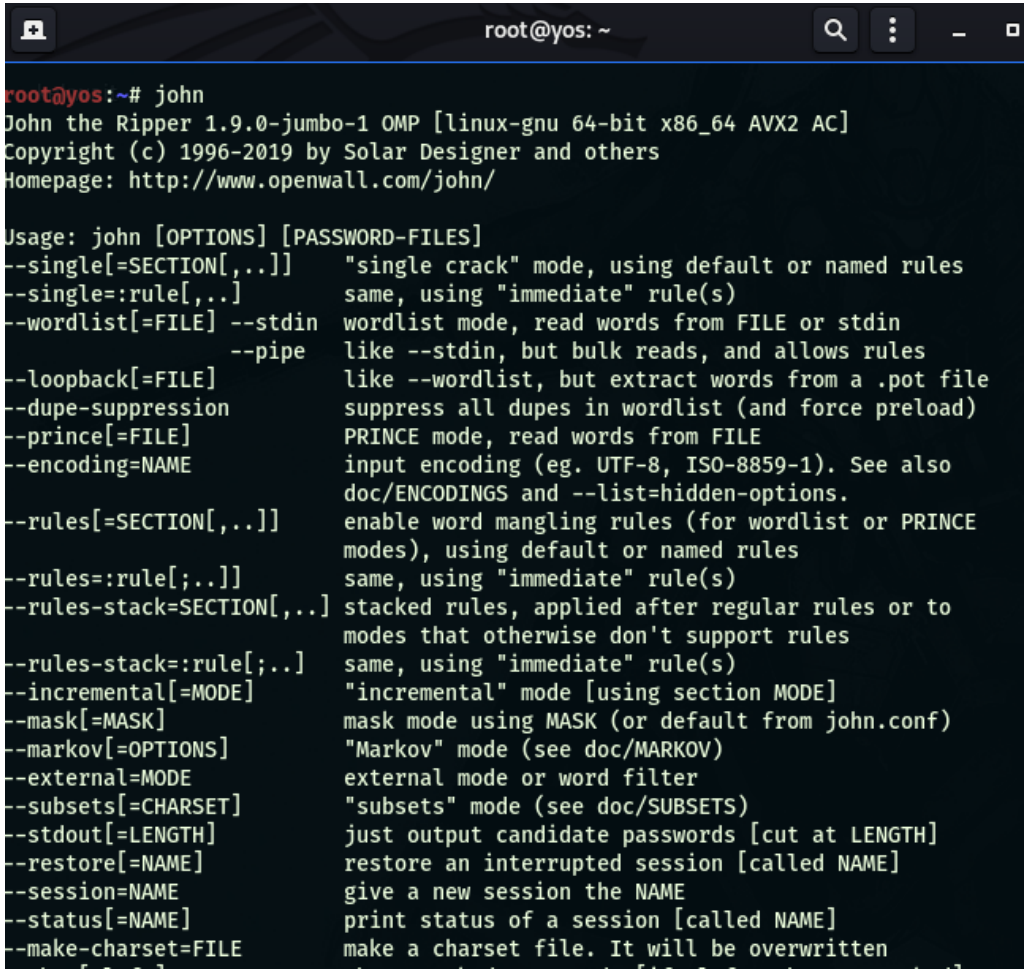
сайт пробивает хэши поддерживаемых форматов по своим вордлистам, определяя наиболее вероятный формат и, в случае нахождения данных, передает первообразную от хэша

> вордлисты

- rockyou.txt
- google-10000-english
- crackstation's password cracking dictionary
- hashesorg
- weakpass
- dchtpassv1.0.txt

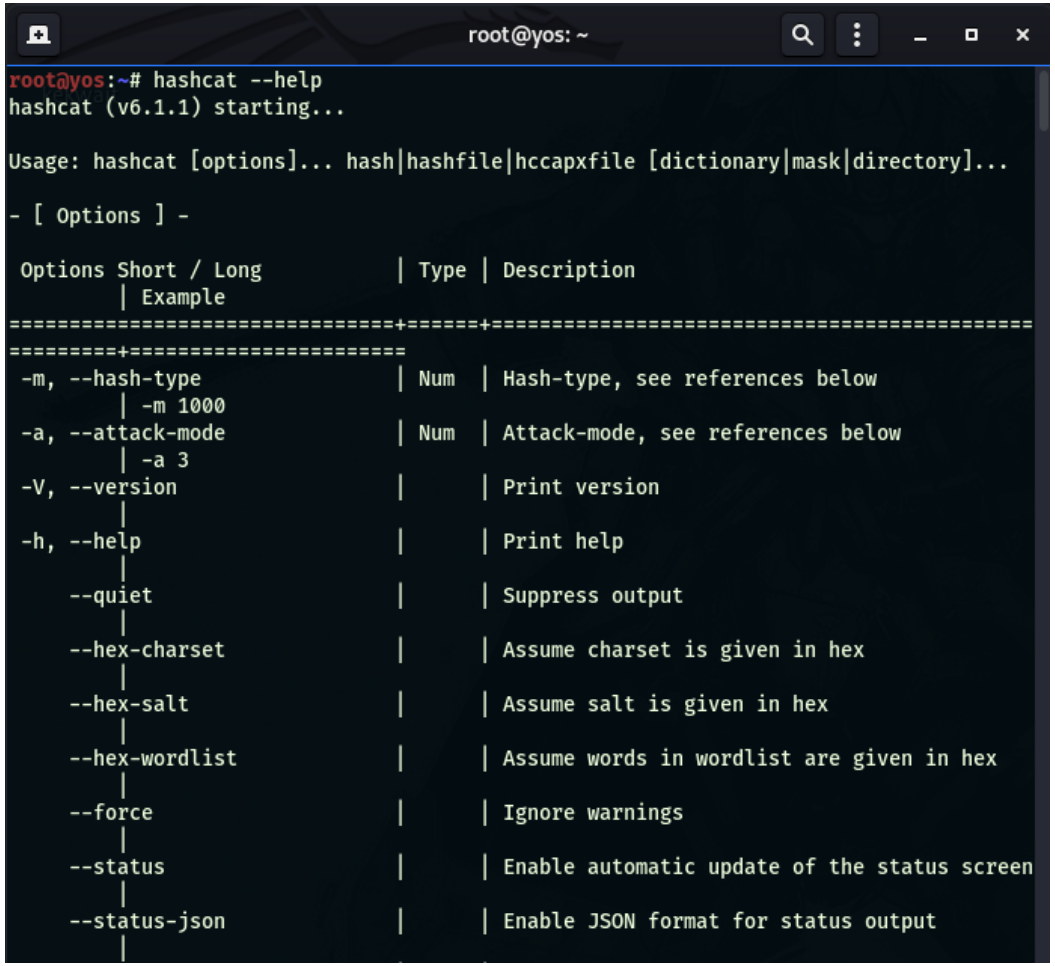
> тулзы для перебора

> john the ripper



john the ripper проводит атаку по словарю и брутфорс. в режиме атаки по словарю программа берёт предполагаемые пароли из указанного файла, генерирует хеш и сверяет его с эталонным. в режиме брутфорса программа перебирает все возможные комбинации пароля.

> hashcat



особенностью hashcat является очень высокая скорость перебора паролей, которая достигается благодаря одновременному использованию всех видео карт, а также процессоров в системе.

> ДЕМО

> demo

- дан запароленный архив и строка ‘215f6ca4fc913f15ff882e3531c8435d’
- понимаем, что это хэш
- пробиваем его на crackstation

Hash	Type	Result
215f6ca4fc913f15ff882e3531c8435d	md5	Wizard$619

- получаем пароль от архива
- внутри архива есть file.txt, открываем его

```
dCBkaWQgZ2l2ZSB0aGUgZGFya25lc3MgYSBzaGFwZeKApgoK4oCcT2gsIG5v4oCdIGhlIGJyZWF0aGVkLgoKQlVUIFlFUywgc2FpZCBEZWF0aC4KClJpbmNld2luZCByb2xsZWQuID
Roc2wzM3B7dzB3XzF0X3c0c19oNHNoIX0KCkZvciBhIG1vbWVudCBoZSB0aG91Z2h0IFdpdGhlbCB3YXMgZ29pbmcgdG8gc3BpdCBoaW0gd2hlcmUgaGUgbGF5LiBCdXQgaXQgd2Fz
IHdvcnNlIHRoYW4gdGhhdC4gSGUgd2FzIHdhaXRpbmcgZm9yIGhpbSB0byBnZXQgdXAuCgrigJxIHNlZSB5b3UgaGF2ZSBhIHN3b3JkLCB3aXphcmQs4oCdIGhlIHNhaWQgcXVpZX
RseS4g4oCcSSBzdWdnZXN0IHlvdSByaXNlLCBhbmQgd2Ugc2hhbGwgc2VlIGhvdyB3ZWxsIHlvdSB1c2UgaXQu4oCdIFJpbmNld2luZCBzdG9vZCB1cCBhcyBzbG93bHkgYXMgaGUg
ZGFyZWQsIGFuZCBkcmV3IGZyb20gaGlzIGJlbHQgdGhlIHNob3J0IHN3b3JkIGhlIGhhZCB0YWtlbiBmcm9tIHRoZSBndWFyZCBhIGZldyBob3VycyBhbmQgYSBodW5kcmVkIHllYX
```

- текст в какой-то кодировке
- декодируем его через cybershef
- находим флаг