

Slovníkový útok

Vojtěch Žák

2022–2023

Požadavky

Program	Verze
Hashcat	6.2.6
John the Ripper	1.9.0

Použité soubory

Název	Popis
password.hash	Soubor obsahuje MD5 hash hesla <i>password</i>
wordlist.txt	Soubor obsahuje 10 nejpoužívanějších hesel

Úvod

Slovníkový útok spočívá ve vyzkoušení hesel z nějakého seznamu, například již prolomených hesel. Je totiž pravděpodobné, že heslo, které se snažíme prolomit, bylo použito vícekrát tím samým člověkem nebo je populární mezi lidmi. Jako příklad můžeme uvést naše příkladové heslo *password*. Zaprvé se jedná o běžné anglické slovo a zadruhé se jedná o jedno z nejpoužívanějších hesel na světě. Právě seznamy nejpoužívanějších hesel jsou typickým příkladem slovníku pro slovníkový útok.

Wordlists

V Kali Linux je speciální příkaz a složka, které nám dávají předpřipravené slovníky z různých zdrojů. Mezi ně patří třeba Wifite, Metasploit nebo samotný John the Ripper. Avšak nejvíce používaný je rockyou. Jedná se o slovník hesel ukradených společností RockYou. Na rozdíl od slovníků například od společnosti John the Ripper, které jsou tvořeny uměle z více zdrojů, slovník rockyou je vyextrahovaná databáze hesel reálných uživatelů jedné firmy.[1]

Všechny tyto slovníky jsou v Kali Linux umístěny ve složce `/usr/share/wordlists/`. Abychom vypsalí všechny slovníky, které jsou dostupné, můžeme buď použít příkaz `ls` nebo použijeme vestavěný příkaz `wordlists`¹. Tento příkaz nepřijímá žádné parametry a můžeme ho spustit z jakékoli složky.

```
wordlists
```

Příkaz nás přesune do složky obsahující slovníky. Zároveň nám vypíše list doporučených slovníků. Vedle samotného názvu je vedle nich i vypsána cesta k nim. Pokud tento příkaz spouštíme poprvé, na posledním řádku dostaneme otázku, jestli chceme rozbalit *rockyou.txt*. Ten je totiž zkomprimovaný, aby nezabíral tolik místa na disku. My chceme dekomprimovat rockyou slovník, takže napíšeme `Y` a zmáčkneme `Enter`. Následně se nám vypíše ten samý list s výjimkou toho, že nám přibyl nový soubor *rockyou.txt*.

Můžeme si všimnout, že příkaz nás přesunul do jiné složky, než v které jsme příkaz spouštěli. Pro navrácení stačí zadat *exit*, díky kterému „vyskočíme“ ven z příkazu `wordlists`.

John the Ripper

U programu John the Ripper stačí pouze specifikovat cestu ke slovníku, aby se přepnul do *Wordlist mode*. V našem případě chceme využít soubor *rockyou.txt*, který se nachází

¹Tento příkaz je dostupný pouze v Kali Linux.

ve složce `/usr/share/wordlists/`. Cesta ke slovníku se udává do argumentu `--wordlist`. Následně pokud známe typ hashe, předáme ho do `--format`. Nakonec dáme cestu k souboru s hesly, která chceme prolomit.[2, 3, 4]

```
john --format=Raw-MD5
     --wordlist=/usr/share/wordlists/rockyou.txt password.hash
```

John the Ripper nijak nemanipuluje a neoptimalizuje slovník, který mu dáme. To má výhodu v rychlejší nastartování útoku. Nevýhoda nastává při samotném prolamování hesla, kdy při špatném slovníku může dojít k poklesu rychlosti, a tudíž prodloužení času prolamování. Abychom se tomuhle vyhnuli, musíme slovník optimalizovat.

Optimalizace slovníku spočívá hlavně ve dvou úkonech. První je seřazení hesel. Pokud hesla seřadíme, program na prolamování hesel může využít různých optimalizací na vypočítávání dalšího hashe hesla ve slovníku a tím zvýšit rychlost prolamování. Slovník seřadíme pomocí nástroje `sort`. Tomu dáme cestu k souboru, který chceme seřadit. Následně řekneme, že výstup se má zapsat do nového souboru. To uděláme pomocí symbolu `>`. [5]

```
sort wordlist.txt > wordlist_sort.txt
```

Druhý krok je zbavení se duplicitních řádků. Některé slovníky mohou obsahovat ta samá hesla vícekrát. To může být způsobeno například spojením více slovníků do jednoho. Tato duplicitní hesla nám avšak zpomalují rychlost prolamování, protože se dané heslo vypočítává a zkouší znova, což je zbytečné. K deduplikaci využijeme nástroj `uniq`. Tomu stejně jako u příkazu `sort` dáme cestu k souboru a zapíšeme výstup do nového souboru.[6]

```
uniq wordlist_sort.txt > wordlist_sort_uniq.txt
```

Tyto dva příkazy můžeme spojit do jednoho. Nástroj `sort` přijímá totiž argument `--unique`. Tím zařídíme, aby se řadily pouze ty řádky, které ještě nejsou ve výstupu. Navíc můžeme místo symbolu `>` použít argument `--output`, kde zadáme cestu k výstupnímu souboru.

```
sort --unique --output=wordlist_sort_uniq.txt wordlist.txt
```

Hashcat

U Hashcat musíme vždy zvolit typ útoku pomocí argumentu `--attack-mode`. My chceme zvolit *Dictionary attack*, takže mu dáme parametr 0. Jako vždy musíme také zvolit typ hashe, který prolamujeme a cestu k souboru, který hash obsahuje. Úplně nakonec přijde cesta ke slovníku.[8, 9]

```
hashcat --attack-mode 0 --hash-type 0 password.hash
        /usr/share/wordlists/rockyou.txt
```

Hashcat na rozdíl od John the Ripper si slovník načte a provede na něm různé optimalizace. To sice zpomalí start útoku, ale zase samotné prolamování hesel bude rychlejší.

Zároveň si na rozdíl od John the Ripper musíme dávat pozor na velikost RAM paměti, kterou načtený slovník bude zabírat. Pokud by totiž slovník byl příliš velký, Hashcat by se mohl odmítnout spustit. Aby se Hashcat spustil, budeme mu muset rozdělit slovník na více kusů a postupně mu je dávat. Nástroj na rozdělení souboru na více částí se v Linuxu nazývá `split`. Tomu předáme argument `--line-bytes` s hodnotou, na jak velké kusy chceme slovník rozdělit. V našem příkladě ho chceme rozdělit na soubory, které budou mít maximální velikost 1 GB. Následně napíšeme cestu k souboru, který chceme rozdělit. Nakonec můžeme napsat předponu pro vygenerované soubory.[7]

```
split --line-bytes=1GB /usr/share/wordlists/rockyou.txt
rockyou_
```

Vygenerované soubory budou pojmenovávány abecedním stylem. To znamená, že nakonec souboru se vždy přidá číslo souboru, ale v abecedním pořadí.

```
rockyou_aa
rockyou_ab
rockyou_ac
...
```

Reference

- [1] Wordlists. *Kali Linux: Penetration Testing and Ethical Hacking Linux Distribution* [online]. Kali Linux, 2023–Mar–08 [cit. 2023–03–18]. Dostupné z: <https://www.kali.org/tools/wordlists/>
- [2] John the Ripper’s cracking modes. *Openwall: bringing security into open computing environments* [online]. Openwall, 2013/05/29 17:57:56 [cit. 2023–03–18]. Dostupné z: <https://www.openwall.com/john/doc/MODES.shtml>
- [3] John the Ripper’s command line syntax. *Openwall: bringing security into open computing environments* [online]. Openwall, 2016/01/21 05:10:00 [cit. 2023–03–18]. Dostupné z: <https://www.openwall.com/john/doc/OPTIONS.shtml>
- [4] John the Ripper usage examples. *Openwall: bringing security into open computing environments* [online]. Openwall, 2019/05/19 15:10:04 [cit. 2023–03–18]. Dostupné z: <https://www.openwall.com/john/doc/EXAMPLES.shtml>
- [5] sort: Sort text files. *The GNU Operating System and the Free Software Movement* [online]. GNU Operating System [cit. 2023–03–18]. Dostupné z: https://www.gnu.org/software/coreutils/manual/html_node/sort-invocation.html
- [6] uniq: Uniquify files. *The GNU Operating System and the Free Software Movement* [online]. GNU Operating System [cit. 2023–03–18]. Dostupné z: https://www.gnu.org/software/coreutils/manual/html_node/uniq-invocation.html
- [7] split: Split a file into pieces. *The GNU Operating System and the Free Software Movement* [online]. GNU Operating System [cit. 2023–03–18]. Dostupné z: https://www.gnu.org/software/coreutils/manual/html_node/split-invocation.html
- [8] hashcat. *hashcat: advanced password recovery* [online]. hashcat [cit. 2023–03–18]. Dostupné z: <https://hashcat.net/wiki/doku.php?id=hashcat>
- [9] Dictionary Attack. *hashcat: advanced password recovery* [online]. hashcat [cit. 2023–03–18]. Dostupné z: https://hashcat.net/wiki/doku.php?id=dictionary_attack