# Password cracking 1

cracking cryptography

232

Challenge status: Available
Challenge flags: 6

V této úvodní úloze k prolamování hesel se studenti naučí různé druhy útoků pomocí nástroje hashcat a vyzkouší si prolomit široce používané hashovací algoritmy.

Theory Flags Handbook Solves Connect

## Assignment

Dostalo se vám pod ruce pár hesel z databáze firmy, kterou pentestujete. Pokuste se je všechny prolomit a tím ukázat firmě, že jejich hesla nejsou bezpečná.

Schopnost prolomit zahashované heslo je důležitou dovedností každého bezpečnostního experta. I když bude server sebelépe zabezpečen, stačí jedno slabé heslo a útočník se ho může jednoduše zmocnit. Je nutné vědět jaká hesla jsou prolomitelná a jaká už ne.

Nejprve je však potřeba porozumět tomu, jak jsou hesla ukládána, neboť to je klíč k jejich prolomení.

Hesla většinu času nejsou ukládána ve své přímé podobě (takzvaně v plaintextu), ale jsou ukládána ve své zahashované formě.

## Přesun do složky exercise

Veškeré věci spojené s úlohou se nachází ve složce `exercise`. Do ní se přesunete pomocí příkazu `cd`.

## Plnění úkolů

Program `hashcat` spuštějte pod uživatelem `student`. **NE**spouštějte ho pod rootem! Také nepoužívejte přepínače pro určení výstupního souboru `-o` a `--output`. Je to z důvodu automatické kontroly úkolů.

Task 01

## Crackování md5 hashe

Prvním úkolem je prolomit md5 hash v souboru `md5hash`. Neočekáváte, že firma bude mít nějak zásadně složitá hesla, takže použijte dictionary attack. Na stroji je pro vás již předinstalovaný hashcat a je připravená zkrácená verze známého `rockyou.txt`. Pokud byste měli problém se splněním úkolu, doporučuji se podívat na kapitolu 'Jak ovládat hashcat'.

**Answer** **+5**

**Answer hasn't been recorded yet**
Answer is detected automatically

Task 02

## Crackování sha1 hashe

Zde se toho moc od prvního úkolu neliší až na typ hashe, kterým je heslo zahashované. Pro zjištění hash codu pro příslušný hash se podívejte na https://hashcat.net/wiki/doku.php?id=example_hashes.

**Answer** **+5**

**Answer hasn't been recorded yet**
Answer is detected automatically

Task 03

## Crackování sha2-256 hashe

Prolomte hash v souboru `sha2-256hash`. Použijte dictionary attack a slovník `rockyou.txt`.

**Answer** **+5**

**Answer hasn't been recorded yet**
Answer is detected automatically

Task 04

## Crackování NTLM hashe

Víte, že heslo v souboru `ntlmhash` je zahashované pomocí NTLM a skládá se z šesti číslic. Použijte mask attack a prolomte heslo.

**Answer** **+5**

**Answer hasn't been recorded yet**
Answer is detected automatically

Task 05

## Crackován hashů pomocí online nástrojů

I kdybyste chtěli sebevíce, s wordlistem, který máte k dispozici, heslo ze souboru sha2-256hash-2 prostě neprolomíte. Pro jednoduchá hesla se často ani nevyplatí puožívat hashcat a nejrychlejší je podívat se, jestli není v nějaké online databázi. Inspirovat se můžete z kapitoly 'Online rainbowtables'.

Odpověď zapište ve formátu `haxagon{heslo}`

**Answer** **+5**

Your answer

Submit

**3** Total attempts

Task 06

## Crackování neznámého hashe

Nejtěžší úkol na závěr. Už trochu víte co a jak s hashcatem a je na čase zkusit něco těžšího. Vaším úkolem je identifikovat hash v souboru `unknownhash` a prolomit heslo. S tím vám pomůže program `hashid`, který už je na zařízení předinstalován. A opět použijte připravený wordlist `rockyou.txt`.

▶ Nápověda

**Answer** **+10**

**Answer hasn't been recorded yet**

Answer is detected automatically