Elektrotehnički fakultet u Beogradu
Katedra za računarsku tehniku i informatiku

Zaštita računarskih sistema i mreža

- Sedma laboratorijska vežba -

7.1. hashcat alat

hashcat (https://hashcat.net/hashcat/) je alat za otkrivanje lozinki na osnovu hash vrednosti. Radi tako što izračunava lozinke poznatih baza lozinki i poredi ih sa zadatim hash-om. Podržava veliki broj različitih hash funkcija koje se koriste u današnjim operativnim sistemima za čuvanje lozinki i ima funkcionalnosti koje omogućavaju hardverska ubrzanja, što ga čini jednim od najpopularnijih alata za otkrivanje lozinki. U okviru ove vežbe će biti pokazan način na koji može da se iskoristi **hashcat** alat za otkrivanje lozinki sačuvanih u različitim formatima i to onih lozinki koje su ranije otkrivene u nekim hakerskim napadima i postoje u snimljenim bazama lozinki. Na virtuelnu mašinu u laboratoriji hashcat se instalira komandom:

```
sudo apt install hashcat
```

Komandom `hashcat -h` mogu da se dobiju sve opcije ove komende, a posebno različite varijante hash algoritama za koje ovaj program može da odredi lozinku.

Postoji puno baza lozinki koje su u različitim trenucima ukradene od brojnih firmi. Decembra 2009 hakeri su ukrali lozinke svih naloga (preko 32 miliona) kompanije RockYou. Kompanija je koristila neenkriptovane fajlove sa lozinkama, a napad je izveden koristeći tada 10 godina star SQL napad. Lozinke koje su tada snimljene sadrže mnoge često korišćene lozinke i mogu da se preuzmu sa ove lokacije: http://downloads.skullsecurity.org/passwords/rockyou.txt.bz2. Druge lozinke zabeležene na istom sajtu mogu da se nađu ovde: https://wiki.skullsecurity.org/index.php/Passwords. Takođe, novije lozinke koje su snimljene tokom hakesrkih napada mogu da se nađu na nekim lokacijama:

- https://github.com/danielmiessler/SecLists/tree/master/Passwords
- https://github.com/yuqian5/PasswordCollection

Zadatak 7.1.1 Otkrivanje lozinke zaštićene LM hash-om

Otkriti lozinku kojom je kreiran sledeći LM hash na starijem Windows operativnom sistemu:
`AC4ACD4E2CA13E80AAD3B435B51404EE`

Poznato je da je korišćena lozinka koja postoji u bazi lozinku koje su 2017 preuzete sa darkweb-a. Prekopirati gornji hash u fajl hash.txt. U isti folder u kojem je hash.txt preneti fajl sa lozinkama preuzetim sa dark weba:

```
wget https://github.com/danielmiessler/SecLists/blob/master/Passwords/darkweb2017-top100.txt
```

Uneti komandu kojom se dobija lozinka iz ovog hash-a:

```
hashcat -m 3000 hash.txt darkweb2017-top1000.txt --force --show
```

Dobiće se korišćena lozinka: **GWERTY**

Zadatak 7.1.2 Otkrivanje lozinke zaštićene NT hash-om

Otkriti lozinku kojom je kreiran sledeći NT hash na Windows operativnom sistemu:
`30EF6BD2540EB0CB7010D769538AEBA8`

Poznato je da je korišćena lozinka koja postoji u bazi lozinku koje su 2017 preuzete sa darkweb-a. Prekopirati gornji hash u fajl hash.txt. Uneti komandu kojom se dobija lozinka iz ovog hash-a:

```
hashcat -m 1000 hash.txt darkweb2017-top1000.txt --force --show
```

Dobiće se korišćena lozinka: **booboo1**

Zadatak 7.1.3 Otkrivanje lozinke zaštićene NTLMv2 hash-om

Otkriti lozinku kojom je kreiran sledeći NTLMv2 hash na Windows operativnom sistemu:
`crackme::HOGWARTS:c341fbf1b979cd7c:4A563CD449DA4A454A34156276EA2BE4:010100000000000080B99E33027FD50145514F334F6572670000000001000A0053004D0042003100320002000E004E004F004D0041005400430048000300 0A0053004D0042003100320004000A0053004D0042003100320005000A0053004D0042003100320007000800 80B99E33027FD50109001400630069006600730002F0053004D0042003100320000000000000000000`

Poznato je da je korišćena lozinka koja postoji u bazi lozinki koje su 2017 preuzete sa darkweb-a. Prekopirati gornji hash u fajl hash.txt. Uneti komandu kojom se dobija lozinka iz ovog hash-a:

```
hashcat -m 5600 hash.txt darkweb2017-top1000.txt --force --show
```

Dobiće se korišćena lozinka: **q1w2e3r4t5y6**

Zadatak 7.1.4 Otkrivanje lozinke zaštićene SHA2-256 hash-om

Otkriti lozinku od koje je dobijen sledeći SHA2-256 hash:
`1C8BFE8F801D79745C4631D09FFF36C82AA37FC4CCE4FC946683D7B336B63032`

Poznato je da je korišćena lozinka koja postoji u bazi lozinku koje su 2017 preuzete sa darkweb-a. Prekopirati gornji hash u fajl hash.txt. Uneti komandu kojom se dobija lozinka iz ovog hash-a:

```
hashcat -m 1400 tryhackme.txt rockyou.txt --force –show
```

Dobiće se korišćena lozinka: **letmein**

Zadatak 7.1.5 Otkrivanje Linux lozinke zaštićene SHA256 hash-om

Otkriti Linux lozinku od koje je dobijen sledeći SHA2-256 hash:
`$5$ToughSalt$pnjWnN3tg7GyY79ao3vYo9ouPG.rVLw9PKitIdlJnK3`

Poznato je da je korišćena lozinka koja postoji u bazi Cain.txt (https://raw.githubusercontent.com/berandal666/Passwords/master/cain.txt). Prekopirati gornji hash u fajl hash.txt. Preuzeti bazu lozinki pomoću:

```
wget https://raw.githubusercontent.com/berandal666/Passwords/master/cain.txt
```

Uneti komandu kojom se dobija lozinka iz ovog hash-a:

```
hashcat -m 7400 hash.txt cain.txt –force –show
```

Dobiće se korišćena lozinka: **quadricotyledonous**

Zadatak 7.1.6 Otkrivanje Linux lozinke zaštićene SHA512 hash-om

Otkriti Linux lozinku od koje je dobijen sledeći SHA512 hash:
`$6$ToughSalt$j2zsBYBhaiqTQigzKVNYUor0.W9ecFy7.ieknZnoorHAVZ1qq0JYrECMj27/Sd/AMISpFvYwkOFUVhbS5Sqp//`

Poznato je da je korišćena lozinka koja postoji u bazi Cain.txt (https://raw.githubusercontent.com/berandal666/Passwords/master/cain.txt). Prekopirati gornji hash u fajl hash.txt. (šta je u ovom hash-u hash, a šta salt?)

Uneti komandu kojom se dobija lozinka iz ovog hash-a:

```
hashcat -m 1800 hash.txt cain.txt --force
```

Nakon što je lozinka pronađena (dobija se poruka “cracked”) uneti:

```
hashcat -m 1800 hash.txt cain.txt --force --show
```

Dobiće se korišćena lozinka: **quadricotyledonous**