Lab 6: Online and Offline Password Guessing

Na ovim lab. vježbama simulirali smo online i offline napade.

Kod online password guessinga napadač komunicira sa serverom, a kada se radi o offline napadu, napadač nije u mrežnoj interakciji sa serverom.

1. online napad

   Trebamo se spojiti na katarinabotic.local pomocu ssh ali nam je potrebna lozinka koju moramo saznati znali smo da ima od 4-6 slova i da su sva mala.

   Ukupno ima 25^4+25^5+25^6 mogucih kombinacija slova→ brute force napadom brzinom 64 pokusaja pogadanja/min bilo bi nam potrebno 7.56 godina. Naredba:

   ```
   hydra -l doe_john -x 4:6:a doejohn.local -V -t 1 ssh
   ```

   Zatim smo koristili već kreirani dictionary u kojem su se nalazile neke odabrani pokušaji za pogađanje lozinke te je ovaj napad puno brži od prethodnog. Naredba:

   ```
   hydra -l doe_john -P dictionary/g1/dictionary_online.txt doejohn.local -V -t 4 ssh
   ```

   Pri čemu: Hydra is **a brute-forcing tool that helps penetration testers and ethical hackers crack the passwords of network services**. Hydra can perform rapid dictionary attacks against more than 50 protocols.

2. offline napad

   Ne trebamo za svaki pokušaj slati upit na server već samo uspoređujemo hash vrijednosti lozinki koje pokušavamo s onim hash vrijednostima koje su zapisane u bazi- one su nam poznate imamo popis korisnika s njihovim hashevima odabrali smo nekog korisnika i njegov hash spremili u dokument. Opet smo vidjeli da je pomoću pripremljenog dictionarya napad brži te smo to proveli naredbom:

   ```
   hashcat --force -m 1800 -a 0 password_hash.txt dictionary/g1/dictionary_offline.txt --status --status-timer 10
   ```

   Pri čemu: Hashcat is a powerful tool that **helps to crack password hashes**. Hashcat supports most hashing algorithms and can work with a variety of attack modes.