

Sigurnost računala i podataka - Lab 6

Simulacija online i offline napada. U online napadima je napadac u komunikaciji sa serverom dok u offline napadima uspoređuje hasheve.

Online napad

Na lokalnom serveru se nalaze nasa korisnicka imena i adrese. Prvo smo se pokusali prijaviti na racun pomocu korisnickog imena, ali je zahtjev odbijen jer ne znamo lozinku. Kako znamo da lozinka ima izmedu 4 i 6 znakova i da su sve mala slova dobijemo $25^4 + 25^5 + 25^6$ kombinacija mogućih lozinki. Možemo ih početi isprobavati pomoću hydra alata, ali to na kraju nema smisla jer bi trajalo doslovno godinama. Zatim preuzmemo pre-computed dictionary te ga iskoristimo u napadu i dobijemo lozinku.

Offline napad

Njega radimo pomoću korištenja hasheva i mape shadows gdje se nalaze hashevi lozinki i lista korisnika. Hash spremamo u datoteku i napad izvršavamo s alatom hashcat. Opet koristimo dictionary za brži napad.