Sigurnost: lab 6 - password guessing

Glavni zadatak danasnjeg laba je bia da se upoznamo sa sigurnim nacinom za pohraniit password

Lab je pocea tako da smo preuzali nase challenge sa lok. datoteke i prvo smo krenili sa online napadima

Nakon sta san nasla svoj docker kontejner, spojila san se na njega i trebala san unijeti nekakav password, par puta san pokusavala uniti drugcije krive passworde

Iz toga smo zakljucili da sustav n eogranicava koliko puta mozemo faliti passsword i bia je super primjer za online napad

Ono sta nan je bilo poznato je to da lozinka ima od 4 do 6 malih slova eng abecede, a to znaci da postoji otp. 25^6 razlicitih kombinacija

Te smo izracunali da bi nam u prosijeku tribalo vise od 7 godina da prevrtimo sve opcije ako imamo 64 pokusaja po minuti sta nije najbolja opcija pa koristimo predefinirane dictionaryije

Pomocu njega sada nam u prosijeku triba samo oko 7 min a pronade lozinku ako kao I u proslom slucaju prelazi 64 opcije po min

Nakon online napada presi smo na offline napad

Imamo pristup zeljenom komp. Ono sta zelimo nac su passwordi drugih korisnika

Prvo sta moramo napravit je nac neki file u kojem se nalaze sve te hashiane lozinke, kada ih pronademo moreamo ih kopirat u neki lok. File i tu nam pomaze alat hashcat

Kao i u proslom slucaju imamo otp. 25^6 razlicitih kombinacija te ako cemo pokusat ovo izvrsit brute force napadom trajalo bi predugo pa cemo opet koristit predefinirasne dictionaryije

Kada smo nasli lozinku mozemo se povezati na to racunalo