# Lab 6

Započeli smo tako što smo se spojili na server i provjerili imamo li instaliranu nmap aplikaciju na računalima. Nmap služi za pregled i „upoznavanje“ s dijelovima mreže na koju smo spojeni. Nakon toga smo se pokušali logirati na našu stranicu na serveru, no nismo imali password za pristup. Zatim smo instalirali aplikaciju hydra koju ćemo koristiti kako bi izveli brute-force online napad kako bi saznali password naše stranice kako bi se mogli prijaviti. Kako znamo da je password između 4 i 6 znakova znamo da je ukupan broj kombinacija jednak 26^4 + 26^5 + 26^6 = 321254128 , s tolikim brojem kombinacija i brzinom provjeravanja od 68 passworda po minuti trebalo bi nam nešto manje od 9 godina da provjerimo sve moguće passworde. Kako je to jako puno vremena pokušali smo i dictionary attack s kojim smo uspjeli pronaći password u nekoliko minuta čime možemo vidjeti da dictionary attack može znatno smanjiti vrijeme i broj mogućih passworda koje treba provjriti ukoliko je dictionary „pametno“ sastavljen.

Nakon što smo izveli online password gessing napad kako bi se logirali na našu stranicu, sada ćemo pokušati offline password gessing napad na nečiju tuđu stranicu uz pomoć hashcat-a. Kako bi mogli izvesti napad pronašli smo hash passworda na serveru i pohranili ga u file. Zatim smo pokušali brute-force offline napad koji bi za ovaj password trajao jako dugo zbog toga što je password sastavljen od 6 malih slova što znači da imamo 26^6 = 308915776 mogučih kombinacija za koje bi nam kao i u prethodnom slučaju trebale godine da isprobamo sve kombinacije, pa ćemo i ovdje pokušati skratiti vrijeme uz pomoć dictionary-ja. Kao i u prethodnom slučaju vrijemo potrebno za pronaći odgovarajući password je smanjeno na nekoliko minuta.