SRP - LAB 6

Za svakog studenta na serveru je podignut račun. Cilj vježbe je pogoditi lozinku za taj račun s lokalnog računala.

Korištene tehnologije:

Nmap ("Network Mapper") is a free and open source utility for network discovery and security auditing.

Hydra is a brute-forcing tool that helps penetration testers and ethical hackers crack the passwords of network services

Poznate informacije o lozinki: 4-6 lowercase letters

Password space: 26^4 + 26^5 + 26^6

Za svaki realni sustav poznata nam je kriptografska hash funkcija koju on koristi za hashiranje lozinki, kao i kod te funkcije.

.

Online password guessing

Korištenjem hydra tool-a pokušavamo brute force-at lozinku (bez korištenja dictionary-ja).

Kako radimo online password guessing, za svaku pokušanu lozinku, šalje se zahtjev na server koji onda radi usporedbu probane lozinke i lozinke zapisane u bazi podataka i u slučaju da je točna lozinka pogođena, dobivamo pristup računu.

Kako ne koristimo dictonary, možemo vidjeti da ovakav pokušaj pogađanja lozinke traje vrlo dugo.

Password space je otprilike **308915776 (26^6)** što, ako pogađamo 1 lozinku u sekundi, se prevodi u 10 godina da ispitamo cijeli password space.

Točnu lozinku brže možemo dobit koristeći pripremljeni rječnik.

Dictionary je pripremljeni skup najčešće korištenih lozinki koje su već unaprijed hashirane poznatom kriptografskom hash funkcijom.

U našem pripremljenom riječniku nalazi se 480 mogućih lozinki i za ispitati sve njih potrebno nam je otprilike 8 minuta (brzinom 1 lozinka/sekundi) tako da vrlo brzo doznajemo lozinku našeg računa i možemo se uspješno logirati.

U realnom svijetu, ovakav napad na lozinke ne bi bilo uspješan jer u pravilu većina sustava ima implementiran sistem koji nakon nekoliko pogrešnih pokušaja blokira pristup accountu na određeni vremenski period.

Zato se koristi offline password guessing.

Offline password guessing

Kako bismo mogli izvesti offline password guessing, trebaju nam (na neki način) biti poznate hash vrijednosti lozinki u bazi.

Tada ne trebamo za svaku pokušanu lozinku slati upit na server (i nema mogućnosti da budemo lock out-ani iz accounta nakon određenog broja pokušaja) nego samo uspoređujemo hash vrijednosti lozinki koje pogađamo s hash vrijednostima koje su nam poznate.

Također možemo napraviti brute force attack, ali to će opet trajati predugo, pa koristimo pripremljeni dictionary.

Ponovno nakon kratkog vremenskog perioda doznajemo lozinku accounta.