IZVJEŠTAJ ZA 6. LABORATORIJSKE VJEŽBE

U ovoj vježbi smo se bavili sa napadima na lozinke, tj online i offline pogađanjima lozinki (*Online password guessing* i *Offline password guessing).*

Napadali smo izolirani server koji je unaprijed bio pripremljen za izvođenje napada. Napade smo izvodili na osnovu znanja o *online* i *offline* *dictionary* napadima.

Vježbu možemo podijeliti na 2 dijela:

# Online password guessing

Vježbu smo izveli koristeći *bash shell* u kojem se nalazio server koji smo napadali. Ali prvo smo morali provjeriti je li dostupan time što smo koristili naredbu *ping* na server. Također smo morali instalirati alat *nmap* koji služi za otkrivanje hostova i usluga na mreži tako što šalje pakete i analizira pristigle odgovore. Preko ssh client-a smo se spojili na server na kojem ćemo izvršiti napad.

Što se tiče samog *passworda* znamo 2 metapodatka, a to su da se lozinka sastoji od malih slova i da je duljine 4-6 karaktera. Bez ovih podataka bilo bi teško izvršiti *brute-force* napad, a budući da ih imamo možemo procijeniti da je potrebno provjeriti približno lozinki što je neizvedivo. Instalirali smo alat *hydra* kako bi ga koristili za izvođenje napada. Proslijedili smo mu određene podatke,a to su username, metapodatci o samoj lozinki, server koji napadamo i klijent koji se koristi.

*# hydra -l <username> -x 4:6:a <your IP address or hostname> -V -t 1 ssh*

*hydra -l doe\_john -x 4:6:a doejohn.local -V -t 1 ssh*

Zatim smo pokrenuli napad te izračunali približno potrebno vrijeme da se napad završi. Budući da je to vrijeme bilo dosta veliko odlučili smo prekinuti *brute-force* napad i pokušati sa korištenjem *online dictionary* napada.

Prvo smo spremili riječnik koji nam je zadan te koji sadržava našu lozinku. Zatim smo ponovo pokrenuli napad korišteći *hydra* alat te smo joj, uz prethodno navedene podatke koje smo proslijedili kod korištenja *brute-force* napada, proslijedili još i adresu riječnika kojeg smo preuzeli.

*hydra -l doe\_john -P dictionary/g1/dictionary\_online.txt doejohn.local -V -t 4 ssh*

*Hydra* alat je uspješno pronašla lozinku, te smo se sa dobivenom lozinkom ulogirali na naš server kako bi dokazali da je napad bio uspješan.

# Offline password guessing

Da bi uspješno izveli *offline* napad potrebo je znati neke podatke o samom *passwordu*, a mi smo u našem slučaju znali *hash* vrijrdnost našeg *passworda*. Za dobivanje *hash* vrijednosti naše lozinke koristili smo alat *hashcat* te smo tu *hash* vrijednost spremili na računalo. I ovdje smo zanli neke metapodatke o *passwordu* a to su da se sastoji od malih slova i da mu je duljina 6 karaktera.

Ponovo smo prvo počeli sa *brute-force* napadomza što smo koristili *hashcat* alat. Shvatili smo da je i u ovom slučaju malo previše lozinki koje je potrebno provjeriti. Napad smo pokrenuli na sljedeći način:

*# hashcat --force -m 1800 -a 3 <password\_hash\_file> ?l?l?l?l?l?l --status --status-timer 10*

*hashcat --force -m 1800 -a 3 hash.txt ?|?|?|?|?|?| --status --status-timer 10*

Zaadali smo mu da koristi *brute-force*  napad, 1800 je oznaka za *hash* funkciju, a ?|?|?|?|?|?| predstavlja format naše lozinke, tj da se ona sastoji od 6 karaktera.

Zatim prelazimo na *offline dictionary* napad. Za izvođenje navedenog napada koristimo rječnik kojeg smo preuzeli na naše računalo. U ovom slučaju ne pokušavamo saznati naš *password* već pokušavamo saznati *password* nekog drugog korisnika. Napad izvodimo pomoću *hashcat* funkcije na sljedeći način:

# hashcat --force -m 1800 -a 0 <password\_hash\_file> <dictionary\_file> --status --status-timer 10

hashcat --force -m 1800 -a 0 password\_hash.txt dictionary/g1/dictionary\_offline.txt --status --status-timer 10

Napad smo izveli uspješno jer smo imali odgovarajući rječnik i jer smo saznali *hash* vrijednost naše lozinke.