IZVJEŠTAJ 6.LABORATORIJSKE VJEŽBE

Na 6.laboratorijskoj vježbi smo se usredotočili na lozinke tj. na online i offline pogađajnje istih. Upotrijebilo smo prethodno stečena znanja o online i offline *dictionary* napadima te smo ta znanja primjenili na ovu vježbu. Server koji smo „napadali“ je bio izoliran i već unaprijed pripremljen za naše napade. Ovu vježbu je najlakše sumirati tako što je pdijelimo na 2 dijela.

1.DIO VJEŽBE- Online password guessing

1.dio vježbe smo direktno tj. online napadali server iz *bash shella.* Ali, prvo smo morali provjeriti da li nam je isti dostupan, a to smo provjerili na način da smo *pingali* server. Ovdje se u vježbi susrećemo sa prvim bitnim alatom: nmap. Nmap se koristi za otkrivanje hostova i usluga na računalnoj mreži slanjem paketa i analizom odgovora. Zatim se preko ssh klijenta spajamo na sami *remote* server na kojem ćemo izvršavati sami napad. Pošto bi *brute-force* napad bio dosta težak bez da postoje neki metapodatci o samom *passwordu,* poznajemo i 2 metapodatka o *passwordu:*

1.sastoji se od malih slova

2.dužine je od 4 do 6 karaktera

Poznavajući ove posdatke, procjenjujemo da bi nam za *brute-force* napad bilo potrebno provjertit približno 25^6 *passworda* koji zadovoljavaju ove kriterije što bi bilo neizvedivo ako provjeravao približno od 200 do 1000 *passworda* svake minute. Za automatizaciju napada smo koristila alat hydra kojem smo dali informaciju o kojem se korisniku radi, koja je duljina samog *passworda*, koji server napada te koji se klijent koristi.

COODE: hydra -l doe_john -x 4:6:a doejohn.local -V -t 1 ssh

Nakon što smo pokrenili sami napad te izračunali prosječno vrijeme koje bi nam bilo potrebno, odustali smo od *brute-force* napada te prelazimo na *dictionary* napad. Lokalno smo spremili riječnik koji smo preuzeli koji je za potrebe vježbe sadržavao naš *password*. Kako bismo saznali naš *password,* ponovno smo upotrijebili hydru kojoj smo još naglasli gdje se nalazi naš riječnik iz kojeg će tražiti *password.*

CODE: hydra -l doe_john -P dictionary/g1/dictionary_online.txt doejohn.local -V -t 4 ssh

Konkretno za moj primjer smo rezultatz dobili:

RESULT: [22][ssh] host: juric-pesicmijo.local login: juric-pesic_mijo password: ispent

Hydra je sada pronašla naš *password* te smo se sa ovim *passwordom logirali* na server nad ojim ćemo sada izvršavati *offline* napad.

2.DIO VJEŽBE- Offline password guessing

Za unčikovit *offline* napad, potrebno je znati neki metapodatak ili nešto što je direktno vezano sa našim *passwordom.* Mi smo u ovom djelu vježbe znali *password hash* što nam je omogučilo *offline* napad. Da saznamo *password hash*, pomogao nam je alat hashcat. Taj smo *password hash* spremili lokalno. I ovdje smo kao kod *online* napada znali neke netapodatke o samom *passwordu:*

1.sastoji se od malih slova

2.duljine je točno 6 karaktera

Pomoću hashcata smo započeli *brute-force* napad, ali kao i u prošlom slučaju shvatili smo da je *passworda* približno 25^6 što je ipak malo previše. Sam smo napad pokrenili slijedećim kôdm.

CODE: hashcat --force -m 1800 -a 3 hash.txt ?l?l?l?l?l?l --status --status-timer 10

Ovime smo mu rekli da koristi *brute-force* napad, 1800 je oznaka *hash* funkcije koju koristimo, a ?l?l?l?l?l?l format u kojem se nalazi naš *password* tj. da se sastoji od 6 malih slova. Nakon ovoga prelazimo na *offline dictionary* napad u kojem koristimo riječnik kojega smo lokalno preuzeli. Za razliku od *online* napada, ovdije ne želimo saznati naš *password,* već nečiji drugi tj. *password* nekog drugog korisnika kojem ćemo moći pristupiti sa našeg računala. Kad smo preuzeli riječnik, započinjemo napada koristeći hashcat na slijedeći način:

CODE: hashcat --force -m 1800 -a 0 password_hash.txt dictionary/g1/dictionary_offline.txt --status --status-timer 10

Ovo je moguće napraviti jer smo imali adekvatan riječnik te smo poznavali hash vrijednosti *passworda.* Za moj napad, napadao sam rock pjevača Alice Coopera te znajući *hash value* njegovog *passworda,* došli smo do samog *passworda:*

HASH:6$ps4c/.DEjQsxuZaY$Kcm2x0tESTnspjT7kvpFSmO66zkL2pTaEj1xsrQeq.R.bRqIEORs0qk9zuFAPQJdrUq2585ezhc.QDW67W8/p/

PASSWORD: aintie