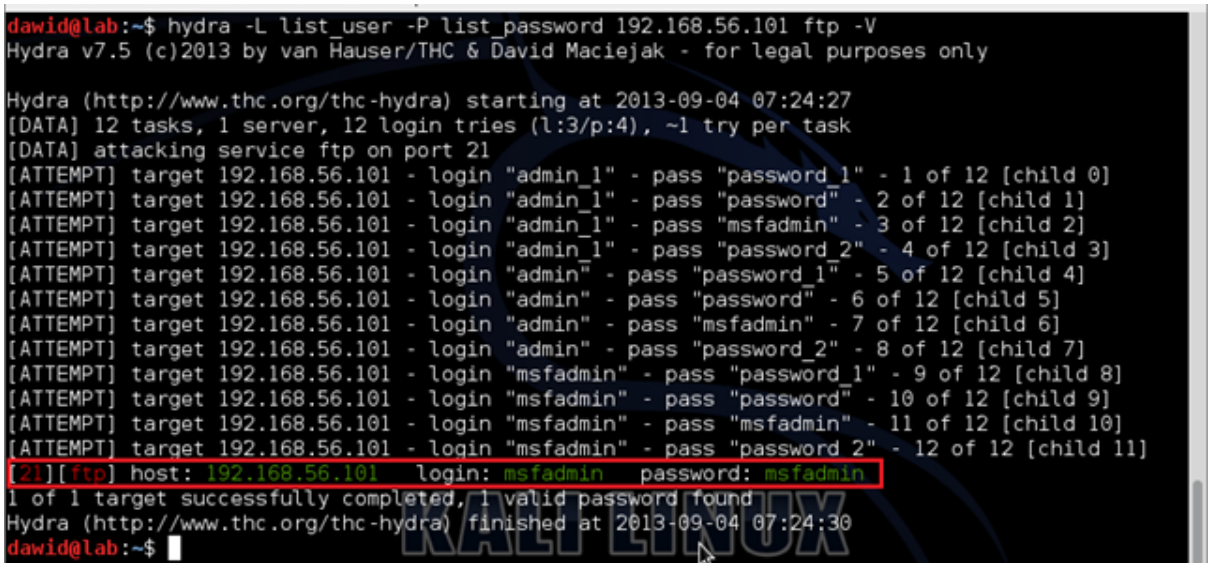


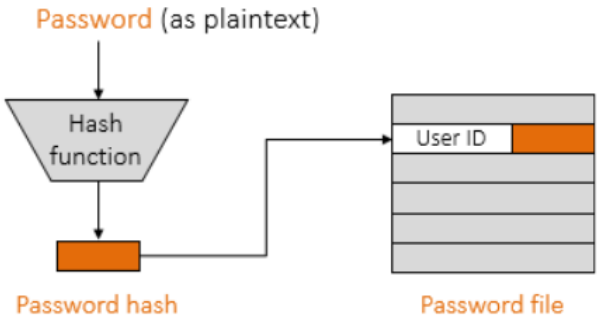
5. laboratorijska vježba: Online and offline password guessing attacks

Studentica: Emilija Sarić

Smjer: 112

Predmet: Sigurnost računala i podataka

→Lozinke su danas najzastupljeniji način autentikacije korisnika, u memoriji se pohranjuje njihova hash vrijednost čime se povećava razina zaštite od krađe i napada.



Slika 1: Način pohrane lozinki pomoću hash funkcije

→Pri napadu napadači mogu provesti online ili offline napad. U online napadu parovi korisničkih imena i lozinki nalaze se na poslužiteljskom serveru. Kod navedenog napada nije potrebno hashiranje lozinki, a server javlja je li lozinka pogođena ili ne. Kod offline napada parovi korisničkih imena i lozinki se također nalaze na poslužiteljskom serveru, a lozinku tražimo po njezinoj hash vrijednosti.

→U ovoj su vježbi izvedeni online i offline napadi na lozinke preko Pre-computed Dictionary napada.

IZVOĐENJE VJEŽBE:

a) ONLINE PASSWORD GUESSING

1. Pokretanje WSL-a i instaliranje nmap-a koji se koristi kao aplikacija za skeniranje IP adresa, portova i detektiranje instaliranih aplikacija u mreži.

2. Preuzimanje personaliziranog korisničkog imena i IP adrese.
3. Pokretanje SSH mrežnog protokola koji korisnicima omogućuje uspostavu sigurnog komunikacijskog kanala između dva računala putem računalne mreža (prvenstveno napravljen zbog remote command line-a) upisivanje linije: `ssh <username>@<your IP address>` .
4. Prema danim podacima računanje broja potencijalnih lozinki (~300 milijuna), pomoću hydra aplikacije provjeravanje vremena potrebnog za proći sve potencijalne lozinke (~ 8 godina).
5. Preuzimanje pripremljenog dictionary-a.
6. Pronalazak lozinke pomoću hydra aplikacije i dictionary-a i logiranje pomoću korisničkog imena i pronađene lozinke: `hydra -l <username> -P dictionary/<group ID>/dictionary_online.txt 10.0.15.1 -V -t 4 ssh`.

b) OFFLINE PASSWORD GUESSING

1. Instaliranje hashcat-a koji se koristi za “probijanje” lozinki, odnosno pronalazk hash vrijednosti lozinke.
2. Preuzimanje hash vrijednosti lozinke drugog računa i pohrana iste lozinke u file u VSC.
3. Pomoću hashcat aplikacije procjena vremena potrebnog za pronalazak hash vrijednosti odgovarajuće lozinke.
4. Preuzimanje pripremljenog dictionary-a za brži pronalazak lozinke.
5. Pronalazak lozinke pomoću hashcat aplikacije i dictionary-a i logiranje pomoću korisničkog imena i pronađene lozinke: `hashcat --force -m 1800 -a 0 <password_hash_file> <dictionary_file> --status --status-timer 10`.

ZAKLJUČAK:

Iz odrađene vježbe može se zaključiti da je brute force napad na lozinke nerealan jer je potrebno previše vremena kako bi se “izvrtile” sve potencijalne lozinke, s druge precomputed dictionary napad puno je prikladniji jer se prolazi samo kroz one lozinke (vjerojatnije, učestalije) koje se nalaze u rječniku te omogućava puno brže izvođenje napada. Također, u ovom se slučaju može zaključiti da je, za zaštitu od dictionary napada, važna što veća entropija lozinki.