Floriana Feminò

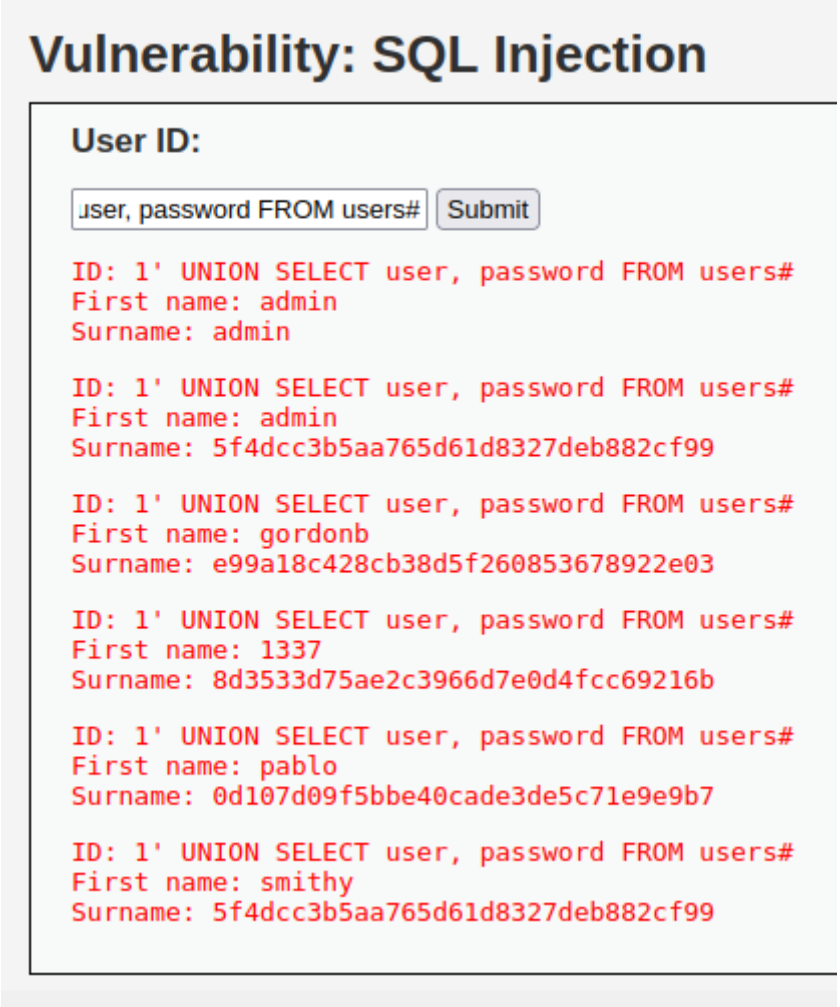
30/11/2022

PASSWORD CRACKING

Task:

Ricavare password dai corrispondenti hash

Utilizzeremo gli hash con algoritmo di cifratura MD5 delle password ricavate da un precedente exploit (ossia una SQL Injection) alla web app di test DVWA:

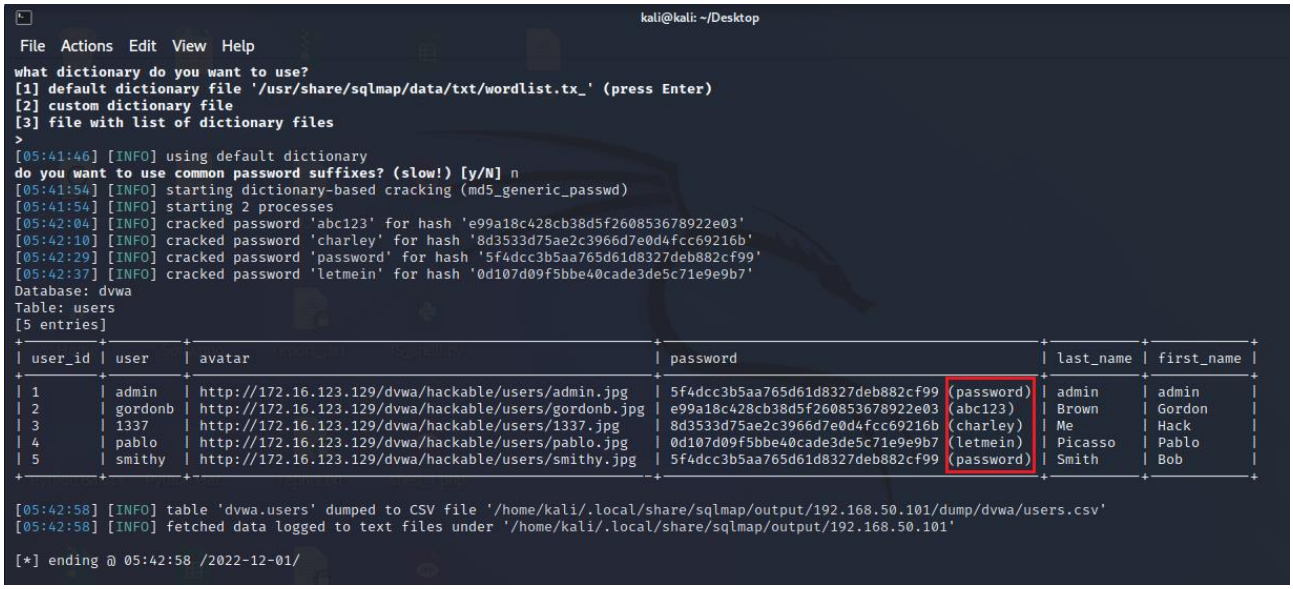


Per far ciò, ci avvarremo di alcuni tool.

1. SQLMAP

Eseguiamo il comando

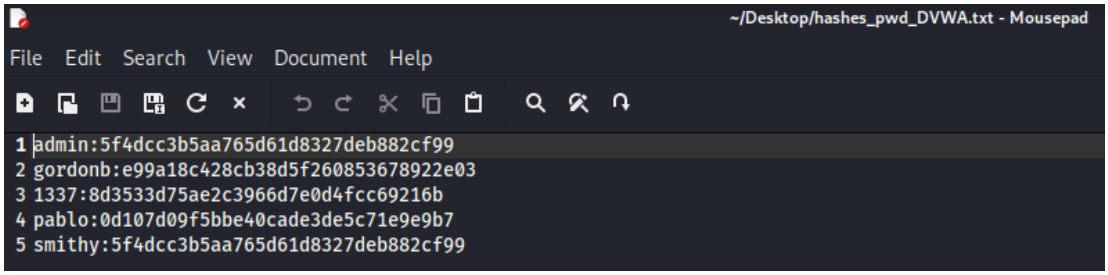
sqlmap -u 'http://192.168.50.101/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit' -cookie='security=low; PHPSESSID=460c8f5e8f3e81ad484089a18c2c03fc' –dump –passwords



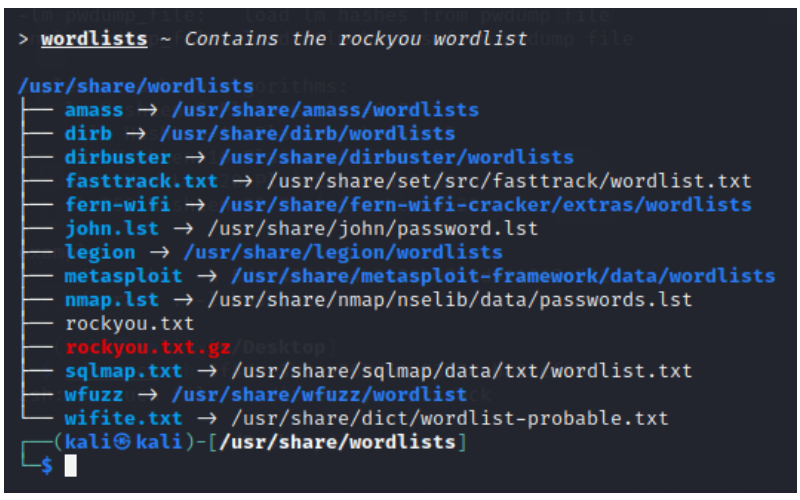
2. John the Ripper

John the Ripper è un tool di password cracking che utilizza la metodologia brute force. Si avvale inoltre di wordlists a scelta dell'utente, utilizzate per attacchi a dizionario.

Per preparare l'attacco, uniamo in un file .txt i nomi utenti della web app appena exploitata insieme agli hash corrispondenti, nel seguente modo:

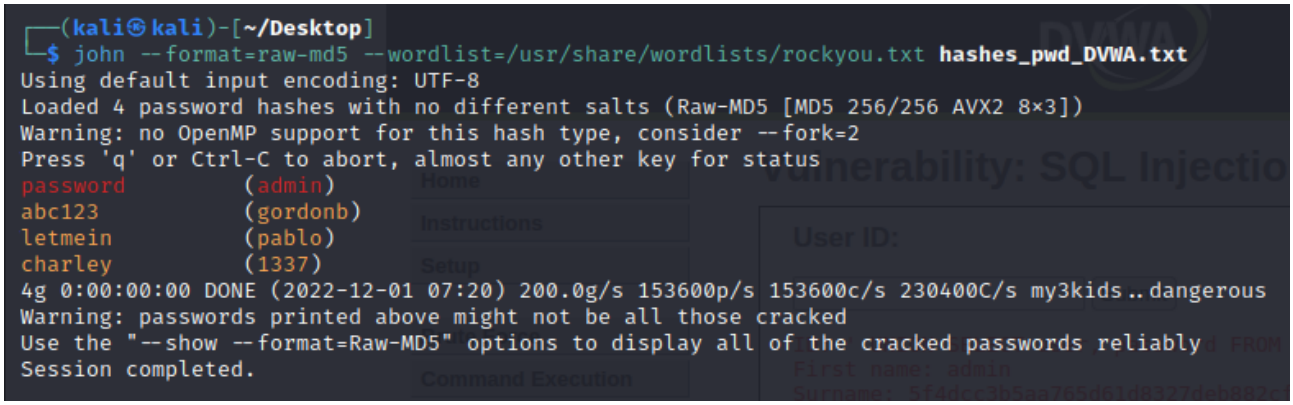


Ora scegliamo una delle wordlists preinstallate in Kali. In questo caso userò **rockyou.txt**



Adesso costruiamo il comando da fornire a JtR. L'input sarà

john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt hashes_pwd_DVWA.txt



Come si può vedere, il tool ha ricavato le password in chiaro degli utenti specificati. Al termine dell'attacco, possiamo usare la funzione show per recuperare i risultati della sessione di cracking, nel seguente modo:

john --show --format=raw-md5 hashes_pwd_DVWA.txt