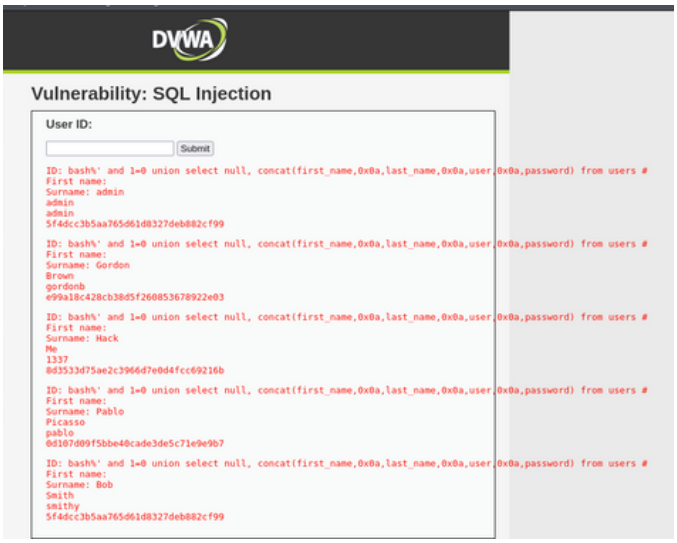
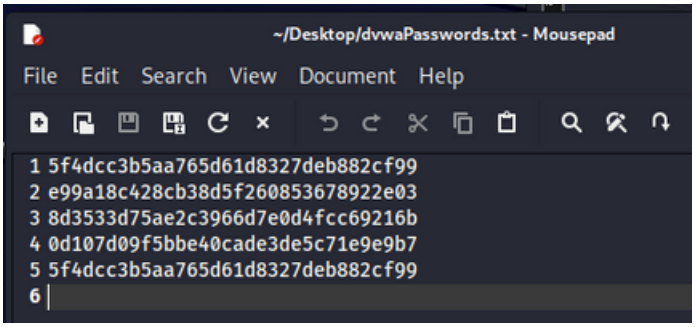
Password cracking

Traccia: password cracking
L'obiettivo dell'esercizio di oggi è craccare tutte le password trovate ieri. Nella lezione pratica di ieri, abbiamo visto come sfruttare un attacco SQL injection per recuperare le password degli utenti di un determinato sistema. Se guardiamo meglio alle password trovate, non hanno l'aspetto di password in chiaro, ma sembrano più hash di password MD5. Recuperate le password dal DB come visto ieri, e provate ad eseguire delle sessioni di cracking sulla password per recuperare la loro versione in chiaro. Sentitevi liberi di utilizzare qualsiasi dei tool visti nella lezione teorica.

Riprendo le credenziali trovate nella precedente esercitazione:

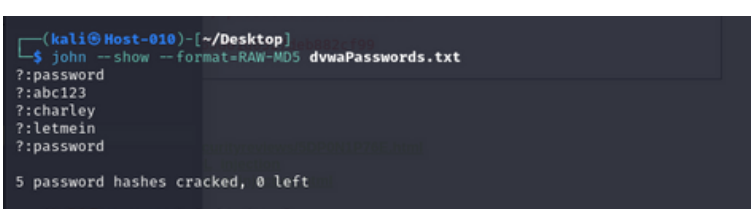


1) **John The Ripper**
Trascrivo su un file .txt le password trovate

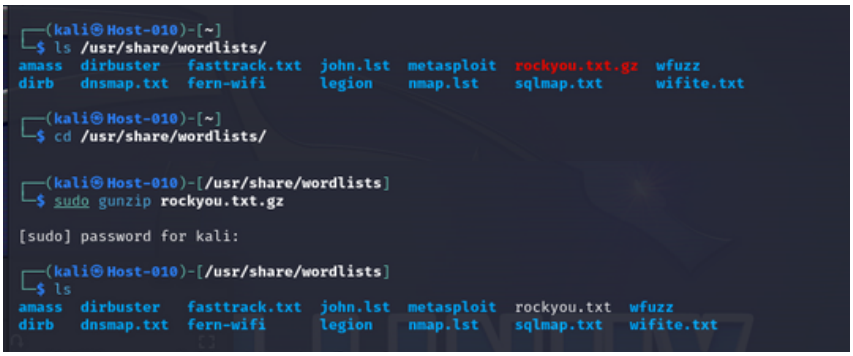


Da terminale utilizzo lo strumento John The Ripper.
Eseguendo il comando *john --format=RAW-MD5 dvwaPasswords.txt* potrò decifrare le password inserite nel mio file .txt

Eseguendo il comando *john --show --format=RAW-MD5 dvwaPasswords.txt* potrò vedere in lista le password trovate.

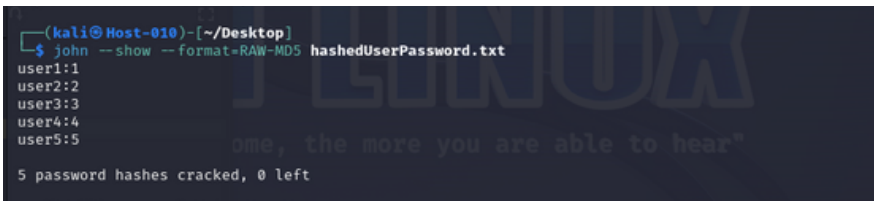


Per tentare un diverso metodo creo un nuovo file .txt contenente le credenziali di 5 user. Le password contenute le ho sottoposte allo stesso procedimento di hashing di quelle proposte da DVWA (MD5).
È possibile sfruttare le wordlists presenti su Kali. Ai fini dell'esercizio scelgo rockyou.txt
Per poterla utilizzare devo prima rimuovere la compressione.



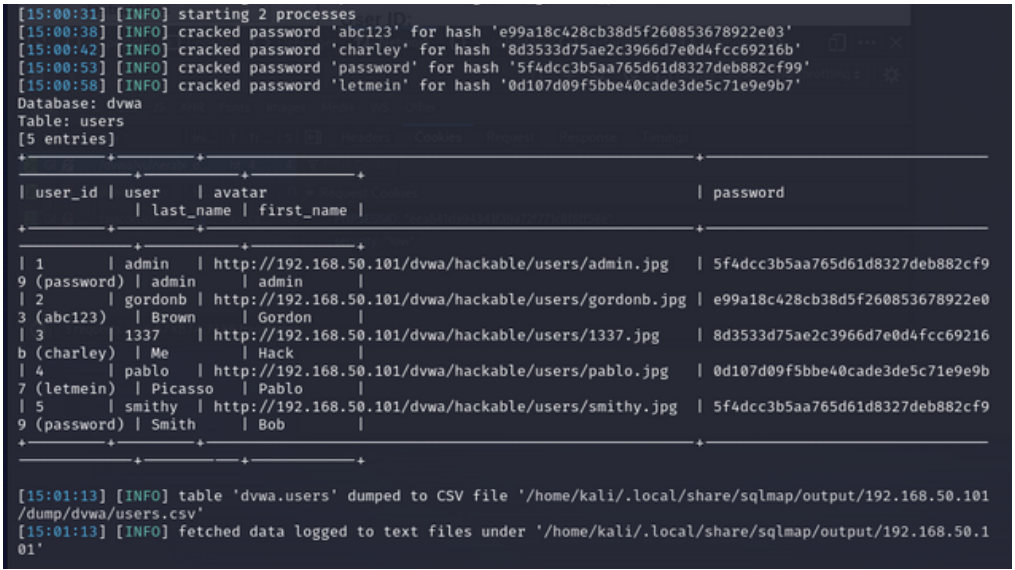
Per decifrare le password eseguo il comando
john --format=RAW-MD5 --wordlist=/usr/share/wordlists/rockyou.txt hashedUserPassword.txt

e a seguire il comando per mostrare la lista abbinata
john --show --format=RAW-MD5 hashedUserPassword.txt



2) SQLMAP

Da terminale su Kali eseguo il comando
sqlmap -u "http://192.168.50.101/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="PHPSESSID=eeab41da94341f39a72f771c8f8ff58e; security=low" --dump -T users --batch



Il comando utilizzato è un esempio di utilizzo di sqlmap, un noto strumento di test di penetrazione che automatizza il processo di rilevazione e sfruttamento di vulnerabilità SQL Injection in applicazioni web.
Analizzando l comando:

- sqlmap: è il comando base per eseguire l'utility sqlmap.
- -u "http://192.168.50.101/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#": questa opzione specifica l'URL da testare. In questo caso, è un URL che punta a una specifica vulnerabilità di SQL injection in DVWA.
- --cookie="PHPSESSID=eeab41da94341f39a72f771c8f8ff58e; security=low": questa parte imposta i cookie necessari per la sessione. PHPSESSID è il cookie di sessione PHP, mentre security=low imposta il livello di sicurezza dell'applicazione DVWA su basso, il che facilita la dimostrazione delle vulnerabilità.
- --dump: questo comando dice a sqlmap di estrarre i dati dal database, una volta trovata la vulnerabilità SQL Injection.
- -T users: questa opzione specifica la tabella da cui estrarre i dati nel database. In questo caso, si sta cercando di estrarre dati dalla tabella users.
- --batch: questa opzione fa sì che sqlmap proceda senza richiedere conferma interattiva per ogni passaggio. È utile per automatizzare l'esecuzione dello script.

Il comando eseguito quindi sta dicendo a sqlmap di testare l'URL specificato per vulnerabilità SQL Injection, utilizzando i cookie forniti, e in caso di successo, di estrarre e visualizzare i dati dalla tabella users del database associato all'applicazione web.