Esercizio del Giorno

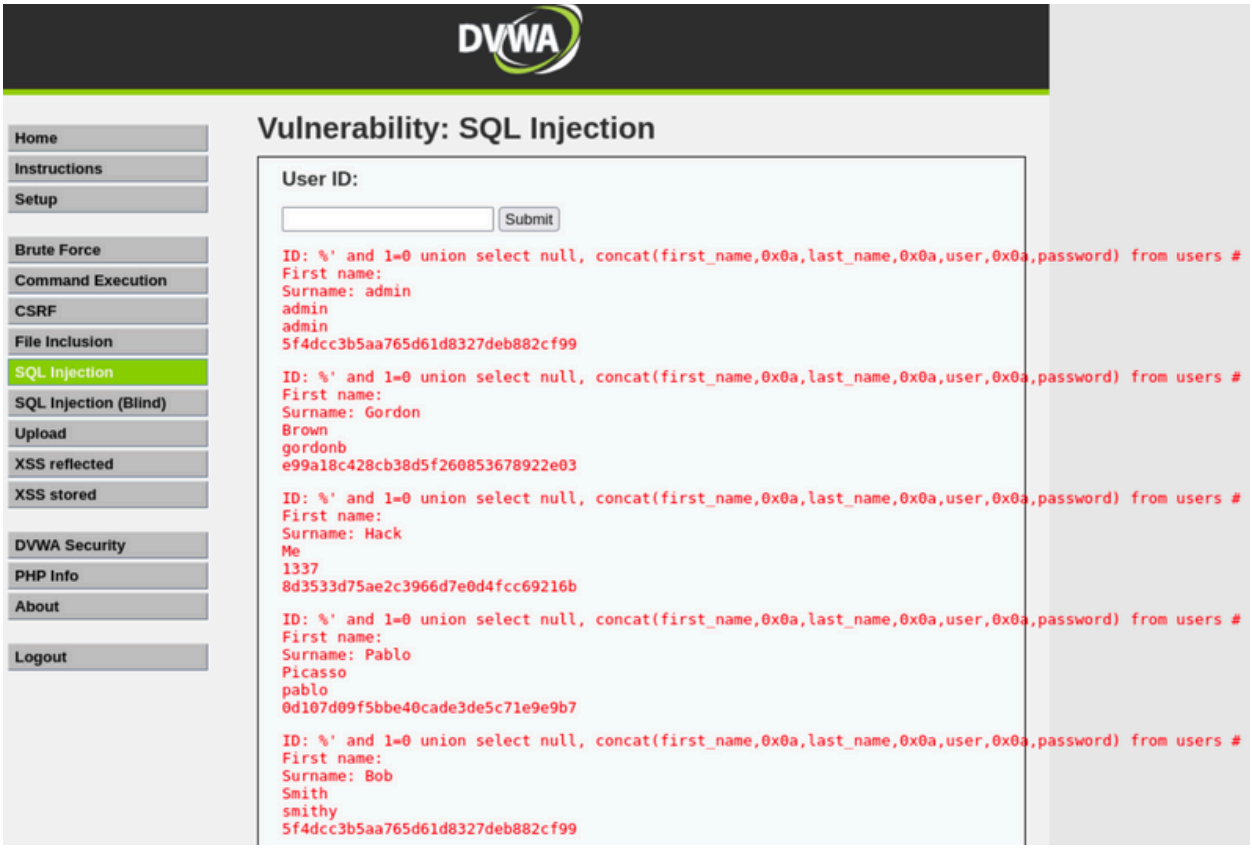
Password Cracking - Recupero delle Password in Chiaro

L'obiettivo di oggi è recuperare le password hashate nel database della DVWA e eseguire sessioni di cracking per recuperare la loro versione in chiaro utilizzando i tool studiati nella lezione teorica.

Risoluzione:

1.Recupero delle Password dal Database:

Una volta creato l'ambiente virtuale con Metasploitable2 e Kali Linux ho effettuato l'accesso alla DVWA di metasploitable. E' stato inizialmente impostato il livello di sicurezza su low e successivamente sotto la voce SQL injection ho inserito il codice seguente per ottenere le credenziali degli utenti:
"" %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users # ""
Una volta ottenute le credenziali è stato creato un file.txt con l'elenco delle password in codice hash da decriptare.



2.Identificazione delle Password Hashate:

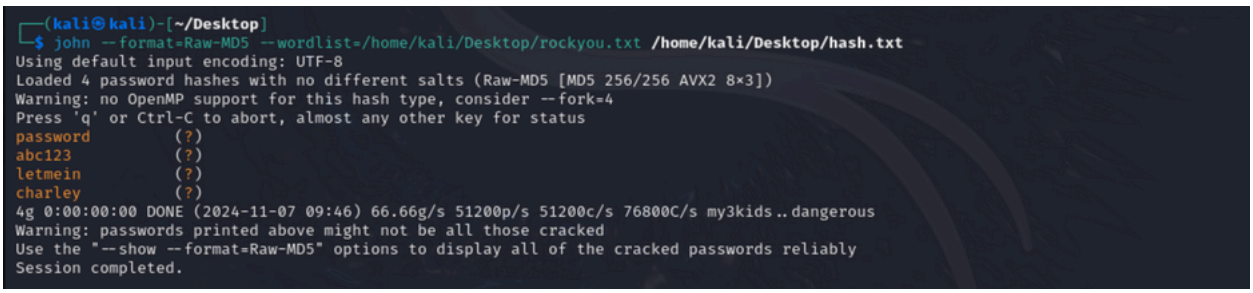
E' stato scritto un programma in Python per identificare il tipo di codice hash, che può essere "MD5", "SHA-1" "SHA-256" "SHA-512". Nel nostro caso il codice in questione è stato identificato come MD5. Un hash MD5 ha una lunghezza fissa di 128 bit, indipendentemente dalla lunghezza dell'input. In termini di rappresentazione esadecimale, questa lunghezza corrisponde a 32 caratteri (16 Byte).

```python
import re

def identify_hash_type(hash_code):
    # Definisci le espressioni regolari per ciascun tipo di hash
    patterns = {
        'MD5': r'^[a-f0-9]{32}$',
        'SHA-1': r'^[a-f0-9]{40}$',
        'SHA-256': r'^[a-f0-9]{64}$',
        'SHA-512': r'^[a-f0-9]{128}$',
    }

    # Controlla ogni tipo di hash
    for hash_type, pattern in patterns.items():
        if re.match(pattern, hash_code):
            return hash_type

    return "Tipo di hash sconosciuto"

# Test del programma
hash_code = input("Inserisci un hash da identificare: ")
hash_type = identify_hash_type(hash_code)
print(f"Il tipo di hash è: {hash_type}")
```

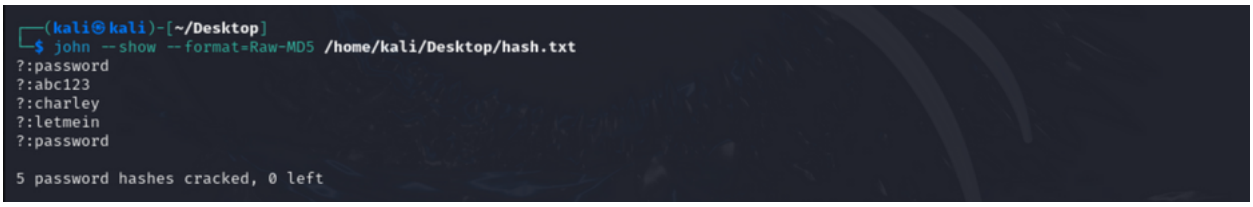
```
┌──(kali㉿kali)-[~/Desktop]
└─$ python identhash.py
Inserisci un hash da identificare: 5f4dcc3b5aa765d61d8327deb882cf99
Il tipo di hash è: MD5
```

3.Esecuzione del Cracking delle Password:

Per decriptare le password in questione utilizziamo John the Ripper che è uno strumento potente e versatile per il cracking delle password, ideale per verificare la sicurezza di sistemi e applicazioni, ma che può anche essere abusato da attaccanti per compromettere account e sistemi vulnerabili. La sua capacità di supportare diversi algoritmi di hash, la velocità di esecuzione e la possibilità di utilizzare attacchi avanzati lo rendono uno degli strumenti di cracking più utilizzati nella sicurezza informatica.
John the Ripper tenta di decifrare gli hash delle password confrontandoli con potenziali password derivanti da un dizionario di parole o tramite attacchi a forza bruta, generando gli hash corrispondenti. Quando trova una corrispondenza, rivela la password in chiaro.



La prima parte del codice [--format=Raw-MD5] indica a John che gli hash nel file da decifrare sono nel formato MD5, infatti Raw-MD5 si riferisce a un hash MD5 "puro" (senza modifiche, senza sale, e senza altre complicazioni). Questo formato è usato per indicare che l'hash da decifrare è una semplice rappresentazione dell'algoritmo MD5.
La parte seguente specifica la wordlist (un dizionario di possibili password) che John userà per tentare di indovinare la password. Ogni parola della wordlist verrà trasformata in un hash MD5 e confrontata con quello fornito nel file degli hash.



L'opzione --show è utilizzata per visualizzare le password decifrate dopo che John the Ripper ha effettuato un attacco e ha trovato una corrispondenza con gli hash nel file di input.
In pratica, questo comando permette di "mostrare" le password che sono state identificate come valide, ovvero quelle che corrispondono agli hash presenti nel file.