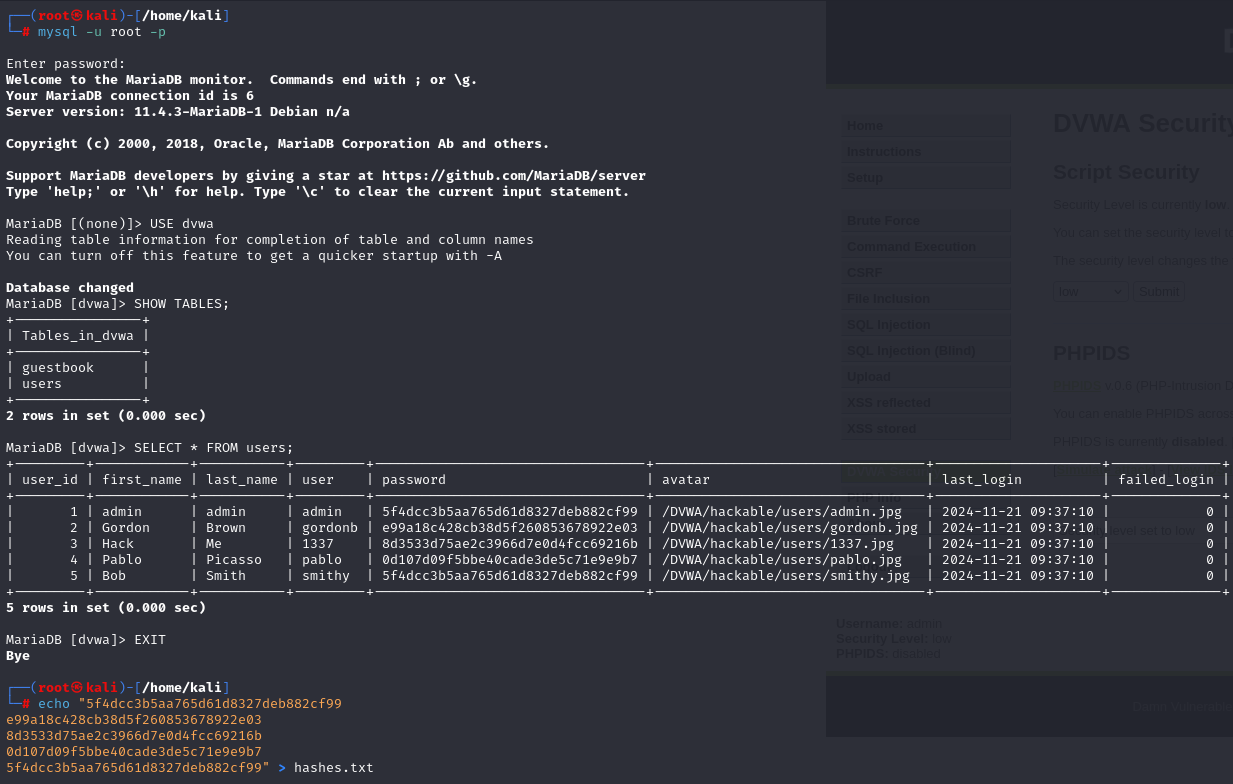
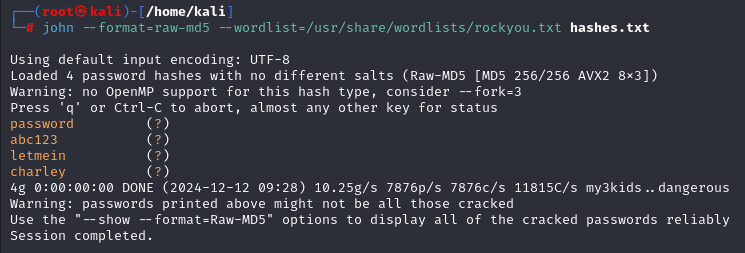
Per recuperare le hashes dvwa ho avviato mysql, gli ho chiesto di usare il database dvwa e di darmi i l’output, ho copiato le hashes e le ho salvate in un file chiamato hashes.txt

Dopo aver installato la wordlist ROCKYOU, ho chiesto a John The Ripper di trovarmi le password:

Le ha trovate nel giro di pochi secondi

Così ho provato con le password extra:

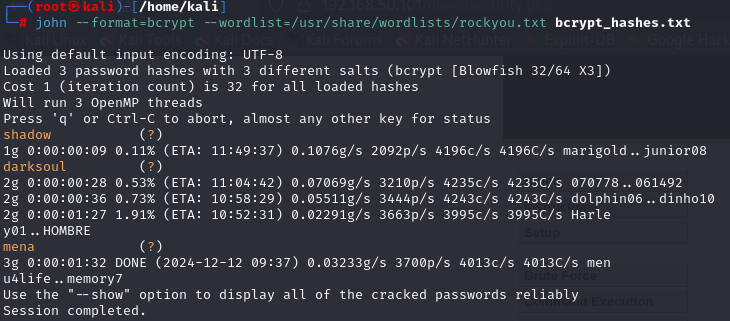
pippo:$2b$05$Ojs/dMUOU12yjrD6OEHJb.cB1zE9CPNg.mPR8BE11f0DIyPaVf436 user:$2b$05$7O7caKmIpPBZxM.RV1lnie/S8jiAjE4C/S6neVAN0ObgJ7tE4dW3. user2:$2b$05$j5vV5M6CMYvUWO9dULw9be29O7RArl9lGIe7ijxf2/47vHwl1YVQq

Visto il prefisso $2b$ ho capito fossero delle password Criptate con algoritmo Bcrypt, molto più lento di MD5 o SHA1.

Per prima cosa ho controllato che la mia versione di JtP supportasse il riconoscimento e cracking di hash bcrypt.

Un altro indizio ce lo dà la sezione $05$, ci specifica il “Costo” della singola hash, bcrypt effettuerà un numero pari a 2^5 di iterazioni prima di generare la hash (32 volte).

Con quest’altro indizio ho potuto dedurre che, sebbene più complesse di quelle precedenti, anche queste 3 password non richiederanno un lavoro troppo estensivo da parte di JtP, così le ho salvate in un file txt e ho lanciato il seguente comando: john --format=bcrypt --wordlist=/usr/share/wordlists/rockyou.txt bcrypt\_hashes.txt

Dopo meno di 5 minuti, questo è il risultato: 

Mi dispiace Akir4d, sei stato John the Ripperizzato