Recuperiamo le password dal database di mysql in codice ash dentro il sito DVWA grazie a una query, sfruttando le sue vulnerabilità come nell’esercizio precedente. Proviamo ora a recuperare la versione in chiaro delle password.

Utilizzeremo il programma John installato di default su kali.

Lista in Ash delle password degli utenti:

ID1 :**5f4dcc3b5aa765d61d8327deb882cf99**

ID2 :**e99a18c428cb38d5f260853678922e03**

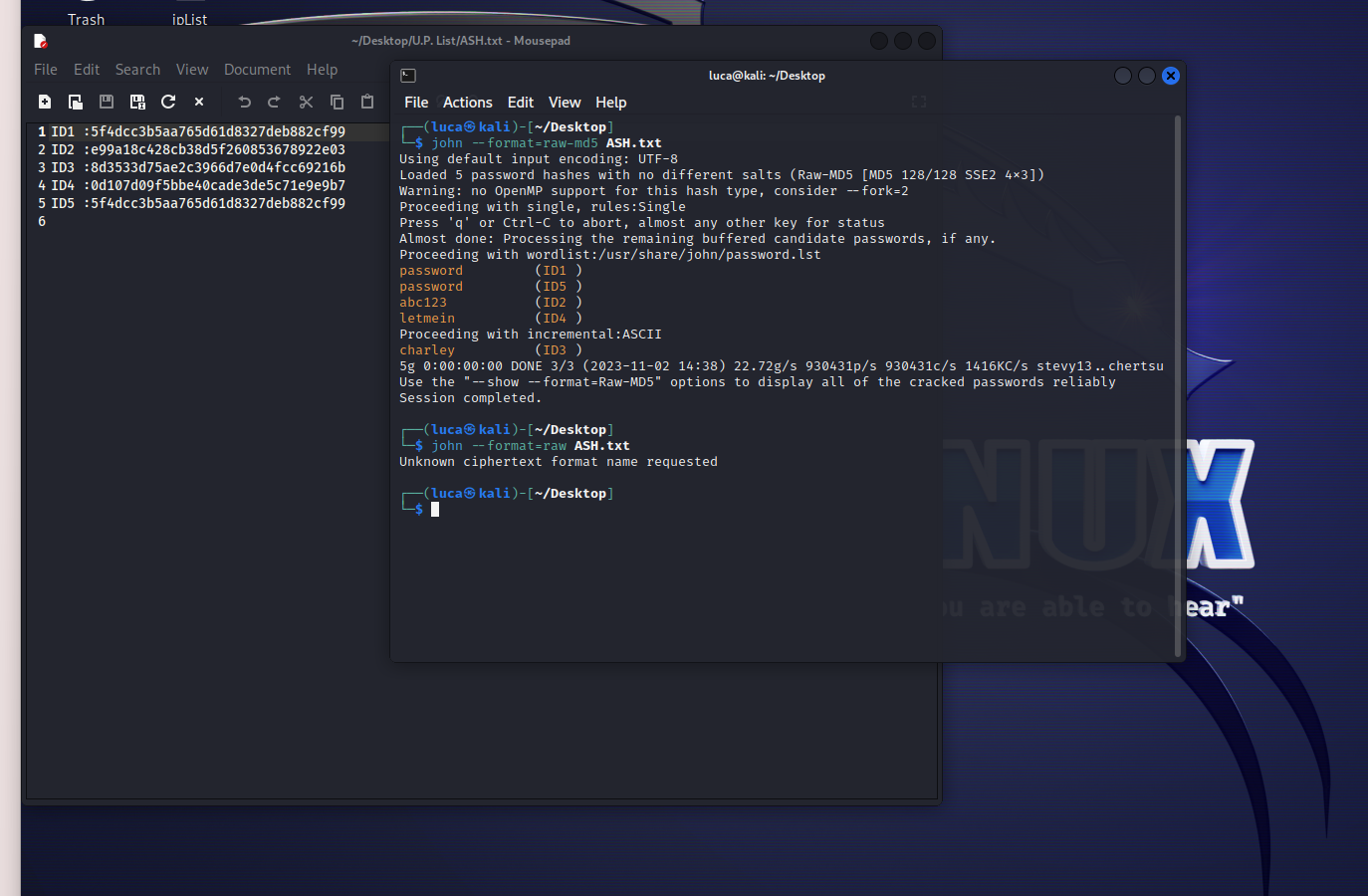
ID3 :**8d3533d75ae2c3966d7e0d4fcc69216b**

ID4 :**0d107d09f5bbe40cade3de5c71e9e9b7**

ID5 :**5f4dcc3b5aa765d61d8327deb882cf99**

Comando utilizzato da terminale **:**

**john –format­­=raw-md5** file\_della\_lista\_da\_utilizzare



John confronterà gli hash datogli in pasto (La nostra lista) e gli hash che genera esso stesso, come risultato finale ci darà le password in chiaro.