STEP-BY-STEP

Wednesday, October 25, 2023 11:47 PM

1. Accesso al DB con utente linux (utente basilare senza permessi di root)
   psql -U linux -d pippo

2. Controllare le tabelle presenti nel DB pippo
   \d

3. Restituire in output il contenuto della tabella utenti
   select * from utenti;

4. Copiare la password hashata ed eseguire il comando hashcat
   Hashcat -a 3 -m 0 pw_hashata

1. Apertura wireshark e accesso alla casella any

2. Filtraggio pacchetti per pgsql

3. Schiacciare pacchetto con lenght 109 e info >p
   //contiene info come nome utente e db di accesso

4. Schiacciare pacchetto con lenght 81 e info <R
   //contiene il sault value

5. Schiacciare pacchetto con lenght 109 e info >p
   //contiene la pw in md5

6. Copiare in un file $postgres$wireshark*sault_value*hash
   //l'hash deve essere senza la parte iniziale md5

7. Far partire il comando hashcat per decriptare la password
   Hashcat -a 3 -m 11100 file.hash

8. Con la password decifrata eseguire l'accesso al db con utente wireshark
   Psql -U wireshark -d pippo