

L'esercizio di oggi consiste nel usare john the ripper per crackare le password hash trovate in /etc/passwd e il file /etc/shadow, e cercare di avere delle password e nomi utenti in chiaro. La prima foto ci fa vedere che le password non sono in grado di craccare.

```
(root@kali)-[/etc]
# john --show passwd
0 password hashes cracked, 0 left
```

La seconda foto ci mostra i due file hash messi insieme che poi useremo per craccare le password e conoscere le password e i nomi utenti.

```
(root@kali)-[/etc]
# unshadow /etc/passwd /etc/shadow
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
_apt:*:42:65534::/nonexistent:/usr/sbin/nologin
nobody:*:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-networkd:*:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesyncd:*:992:992:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus:*:100:102::/nonexistent:/usr/sbin/nologin
tss:*:101:104:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:*:102:65534::/var/lib/strongswan:/usr/sbin/nologin
tcpdump:*:103:105::/nonexistent:/usr/sbin/nologin
usbmuxd:*:104:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:*:105:65534::/run/ssh:/usr/sbin/nologin
dnsmasq:*:106:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
avahi:*:107:108:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
speech-dispatcher:*:108:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
pulse:*:109:110:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
lightdm:*:110:112:Light Display Manager:/var/lib/lightdm:/bin/false
saned:*:111:114::/var/lib/saned:/usr/sbin/nologin
polkitd:*:991:991:polkit:/nonexistent:/usr/sbin/nologin
rtkit:*:112:115:RealtimeKit,,,:/proc:/usr/sbin/nologin
colord:*:113:116:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
nm-openvpn:*:114:117:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
nm-openconnect:*:115:118:NetworkManager OpenConnect plugin,,,:/var/lib/NetworkManager:/usr/sbin/nologin
```