Cracking e Bruteforcing

Creato un file pwds.txt con le password e gli hash

```
└─$ cat pwds.txt
eser1:x:1003:1003:,,,:/home/eser1:/bin/bash
eser1:$6$ib4iK6iItGvL1NIE$BVsxQzq.mmepXdCTP4zFJlDcDxLaclYLTfgL3aIo8ZogWlM.BNNpmdJfPuWh69d/n2XnPpYAattoC9r2zP7kL/:19
052:0:99999:7:::

tulipano:x:1005:1005:,,,:/home/tulipano:/bin/bash
tulipano:$6$jBOf0K5/ymFabsrr$E66i753AHnc7A8YB1rIJA0nL2Qe12XD/hrqyuYaPgbNO/NYX1JE4s5Y5bmhnrFJyX.S3DG7tQuWicv7pJjUou/
:19052:0:99999:7:::

tim:x:1002:1002:Sir Tim Berners-Lee,,,,Inventor of the www:/home/tim:/bin/bash
tim:$6$4mnKuGkT$.mMjEJNNRu5HKhKz3byLHT8GHHTA6xfsiavBWCB8QL8qyJW2BEICTZ6IzRFhRYUNv9PXc/obOtv475WHe.wPm.:19792:0:9999
9:7:::
```

Per la password dell'account **eser1** è bastato andare nella cartella /run di /JohnTheRipper e farlo partire

```
└─$ sudo ./john /home/kali/Desktop/es_cracking/pwds.txt
```

```
└─$ sudo ./john /home/kali/Desktop/es_cracking/pwds.txt --show
eser1:1a2b3c4d:19052:0:99999:7:::
```

Per la password dell'account **TIM**, è bastato fare OSINT in rete per avere informazioni su Tim Berners-lee. Con cupp -i abbiamo inserito tutte queste informazioni e generato una wordlist tim.txt. Poi abbiamo lanciato John che ha trovato la password.

```
┌──(kali㉿kali)-[~/JohnTheRipper/run]
└─$ sudo ./john --wordlist=/home/kali/SecLists/Passwords/tim.txt /home/kali/Desktop/es_cracking/pwds.txt
```

```
┌──(kali㉿kali)-[~/JohnTheRipper/run]
└─$ sudo ./john /home/kali/Desktop/es_cracking/pwds.txt --show
eser1:1a2b3c4d:19052:0:99999:7:::
tim:ecilA&**:19792:0:99999:7:::
```

Cracking di uno zip.

Usiamo l'eseguibile zip2john per andare a creare il file .hashes contenente gli hash da crackare.

```
┌──(kali㉿kali)-[~/JohnTheRipper/run]
└─$ ./zip2john /home/kali/Desktop/es_cracking/es.zip > /home/kali/Desktop/es_cracking/zip.hashes
```

Sarà formato in questo modo:

```
┌──(kali㉿kali)-[~/JohnTheRipper/run]
└─$ cat /home/kali/Desktop/es_cracking/zip.hashes
es.zip:$pkzip$2*2*1*0*0*24*4e04*98c280d94782127ce0a7f049de50345e65f935437d2041d8ace42ed14f723d88827b4471*2*0*29*1d*
f832bddd*81*44*0*29*4e0d*9adf3658d2f9a4597eff986e1e0118b40ac06e9fb5a04c526c4a3f88ed70dd249c75c9b1af0d79e7dc*$/pkzip
$::es.zip:id_rsa.pub, id_rsa:/home/kali/Desktop/es_cracking/es.zip
```

A questo punto lanciamo john in modalità normale (almeno che non abbiamo altre informazioni)

```
┌──(kali㉿kali)-[~/JohnTheRipper/run]
└─$ sudo ./john /home/kali/Desktop/es_cracking/zip.hashes
```

```
Proceeding with wordlist:./password.l
Enabling duplicate candidate password
batman           (es.zip)
1g 0:00:00:00 DONE 2/3 (2024-05-20 05
Use the "--show" option to display al
```

Andiamo ad inserire la pw nel momento in cui facciamo unzip e ne vediamo il contenuto.

Password Recovery (Trovare la password per estrarre un .rar)

Dato che il file è stato generato da ulisse.unibo.it, generiamo una Wordlist con `cewl`

```
┌──(kali㉿kali)-[~/Desktop/es_cracking]
└─$ cewl -d 1 -m 5 https://ulisse.unibo.it > wordlist.txt
```

Andiamo a generare un file di hash in questo modo

```
┌──(kali㉿kali)-[~/JohnTheRipper/run]
└─$ sudo ./rar2john /home/kali/Desktop/es_cracking/crack_esercitazione.rar > /home/kali/Desktop/es_cracking/rar.has
h
```

Andiamo quindi ad usare la wordlist per lanciare john sul file di hash

```
┌──(kali㉿kali)-[~/JohnTheRipper/run]
└─$ sudo ./john /home/kali/Desktop/es_cracking/rar.hash --wordlist=/home/kali/Desktop/es_cracking/wordlist.txt
Using default input encoding: UTF-8
Loaded 1 password hash (RAR5 [PBKDF2-SHA256 256/256 AVX2 8x])
Cost 1 (iteration count) is 32768 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
cyberchallenge   (crack_esercitazione.rar)
```

Estrarre un .rar: `unrar e crack_esercitazione.rar`