MODULO 4 PRATICA - PASSWORD CRACKING

Traccia: password cracking Esercizio Password cracking Abbiamo visto come sfruttare un attacco SQL injection per recuperare le password degli utenti di un determinato sistema.

Se guardiamo meglio alle password trovate, non hanno l'aspetto di password in chiaro, ma sembrano più hash di password MD5.

Recuperate le password dal DB come visto, e provate ad eseguire delle sessioni di cracking sulla password per recuperare la loro versione in chiaro.

Sentitevi liberi di utilizzare qualsiasi dei tool visti nella lezione teorica. L'obiettivo dell'esercizio di oggi è craccare tutte le password trovate precedentemente.

Consegna:

1. Screenshot dell'SQL injection già effettuata

2. Due righe di spiegazione di cos'è questo cracking (quale tipologia / quale meccanismo sfrutta)

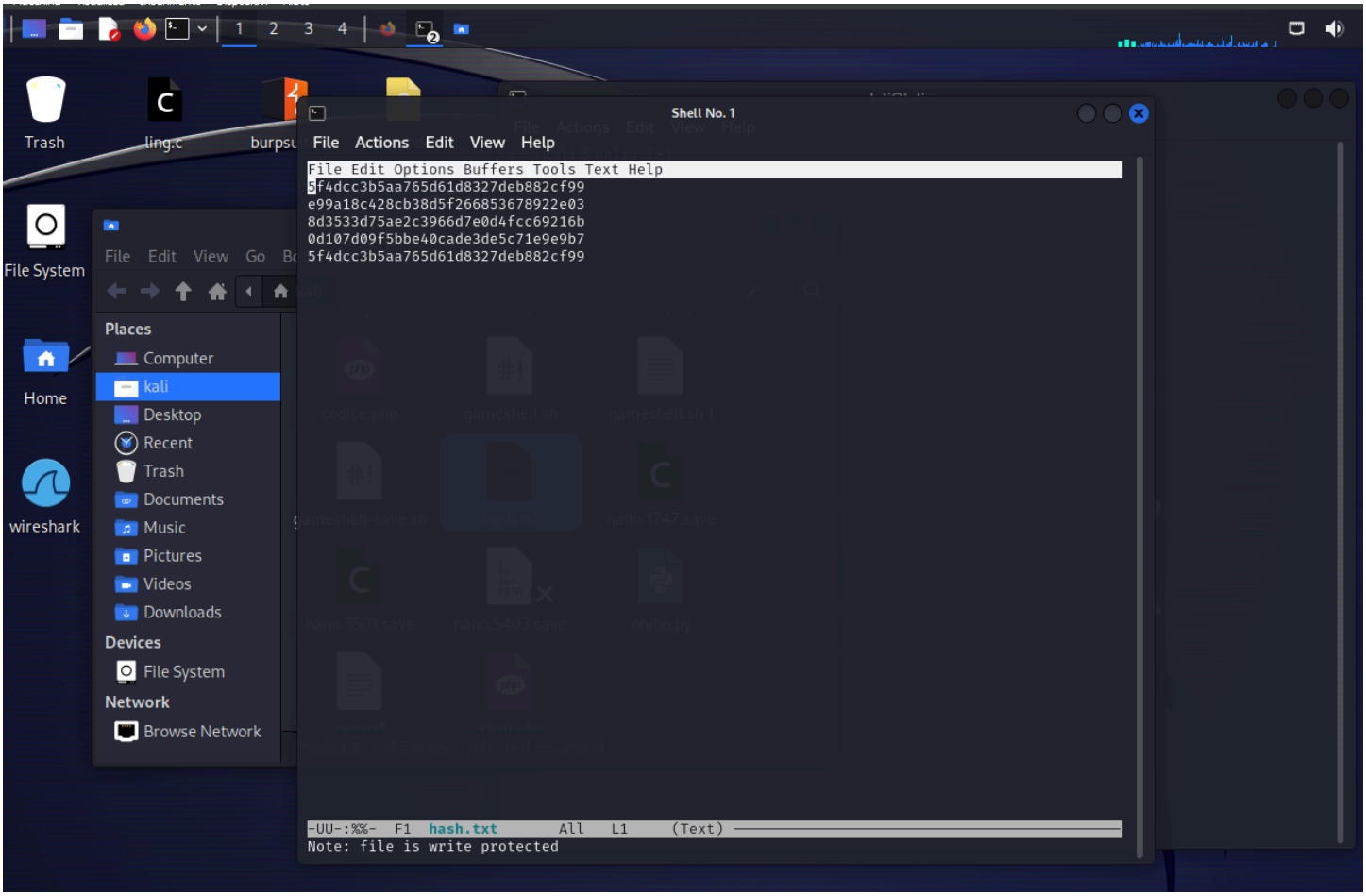
3. Screenshot dell'esecuzione del cracking e del risultato

SVOLGIMENTO

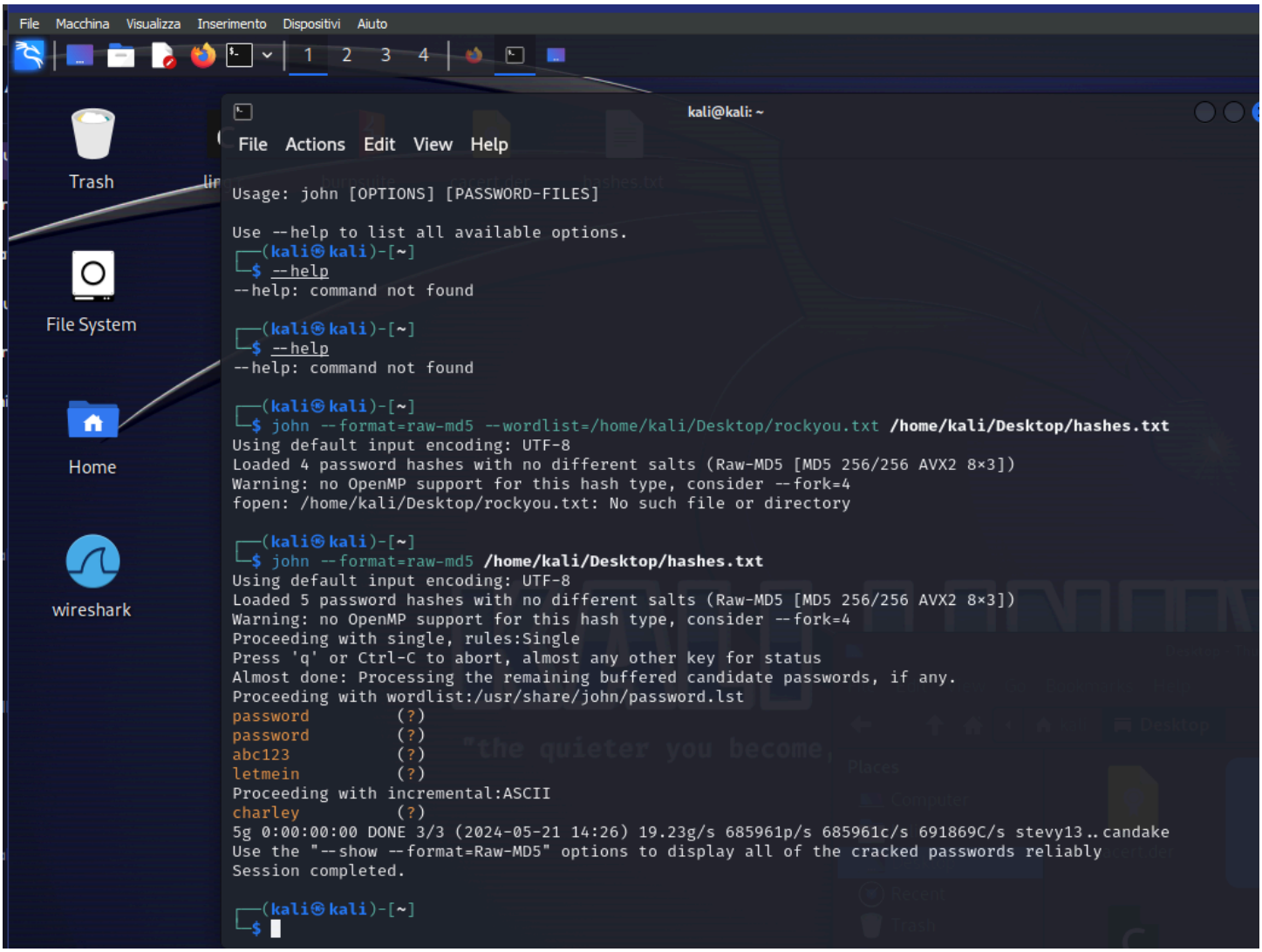
Ecco i nomi utente e le password recuperate con l'SQL Injection:

admin	admin
admin	5f4dcc35aa765d61d8327deb882cf99
gordonb	e99a18c428cb38d5f266853678922e03
1337	8d3533d75ae2c3966d7e0d4fcc69216b
pablo	0d107d09f5bbe40cade3de5c71e9e9b7
smithy	5f4dcc3b5aa765d61d8327deb882cf99

- Per svolgere questo esercizio ci serviremo di John The Ripper.
- Creiamo innanzitutto un file "dizionario" per John The Ripper, inserendo gli hash individuati all'interno di un file txt denominato "hash.txt".



- Procediamo con l'avvio di John the Ripper.
- Per craccare la password con John The Ripper dobbiamo per prima cosa definire il tipo di cifratura da considerare, in questo caso si tratta di un hash in MD5:
  "john --format=raw-md5"
  Avendo già a disposizione le password da craccare, possiamo inserire direttamente il file con su scritte le hash come "dizionario" come punto da cui estrapolarle:


File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
Trash
File System
Home
wireshark
kali@kali: ~
File Actions Edit View Help
Usage: john [OPTIONS] [PASSWORD-FILES]
Use --help to list all available options.
┌──(kali㉿kali)-[~]
└─$ --help
--help: command not found
┌──(kali㉿kali)-[~]
└─$ --help
--help: command not found
┌──(kali㉿kali)-[~]
└─$ john --format=raw-md5 --wordlist=/home/kali/Desktop/rockyou.txt /home/kali/Desktop/hashes.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=4
fopen: /home/kali/Desktop/rockyou.txt: No such file or directory
┌──(kali㉿kali)-[~]
└─$ john --format=raw-md5 /home/kali/Desktop/hashes.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=4
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password (?)
password (?)
abc123 (?)
letmein (?)
Proceeding with incremental:ASCII
charley (?)
5g 0:00:00:00 DONE 3/3 (2024-05-21 14:26) 19.23g/s 685961p/s 685961c/s 691869C/s stevy13..candake
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
┌──(kali㉿kali)-[~]
└─$