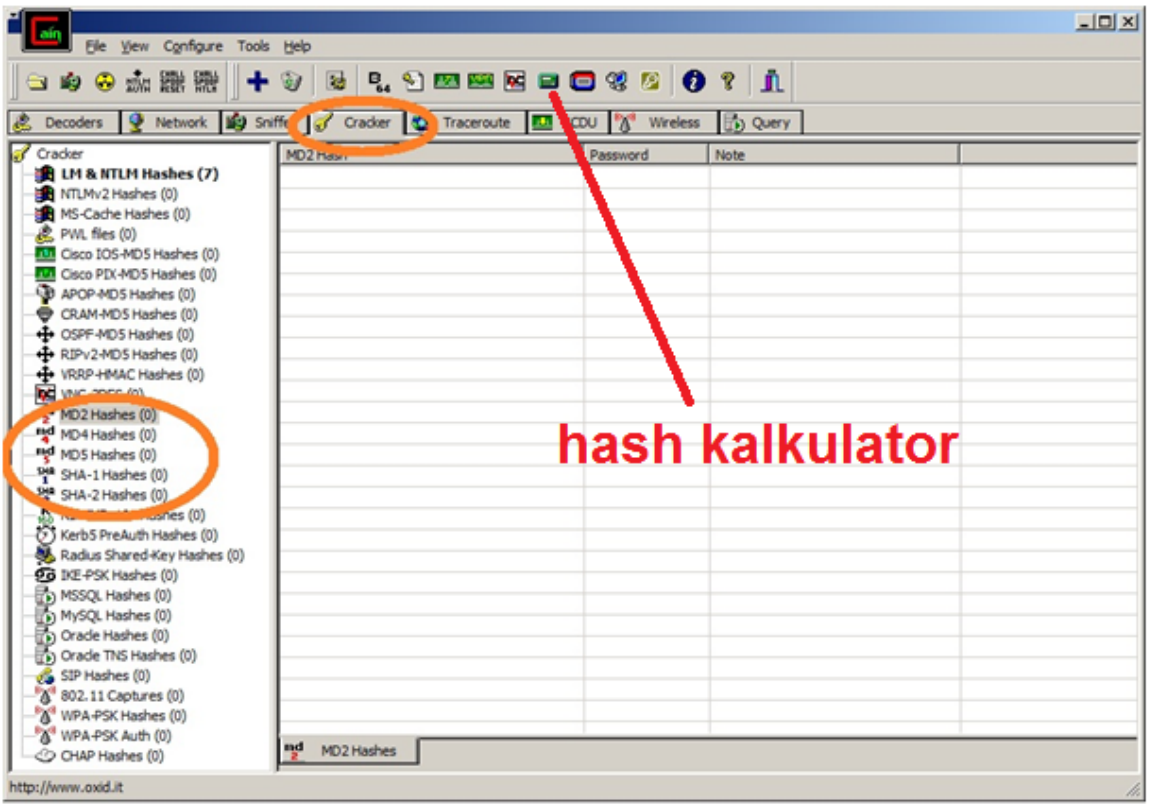
Napadi na gesla

Namen vaje je ugotoviti varnost gesel pri različnih napadih nanje. Napade bomo izvajali s pomočjo programa Cain & Abel.

Namestitev programa Cain & Abel

V mapo ***c:/program files/*** namestite program *Cain & Abel*, ki ga najdete na http://www.oxid.it/downloads/ca_setup.exe

Spodnja slika prikazuje okno progama Cain. Izberite zavihek »Cracker« (razbijalec).



Tvorjenje odtisov

Odtis gesla lahko tvorite s pomočjo »Hash kalkulatorja« (glej gornjo sliko).

Napadanje gesel

V levem oknu razbijalca izberite algoritem, po katerem je bil odtis tvorjen. Nato v seznam na desni dodajte odtis z uporabo gumba  , ki ga najdete v orodni vrstici. Z desnim miškinim gumbom kliknite na izbrani odtis in izberite želeno metodo napada.

Učinkovitost napadov na gesla je odvisna od uporabljene procesorske moči in količine pomnilnika. Poiščite in zapišite si vrsto in hitrost procesorja ter količino pomnilnika vašega računalnika.

Napad s surovo silo

V okviru napada s surovo silo bomo opazovali, kako na razkrivanje gesel vplivajo

- dolžina gesla,
- algoritem tvorjenja odtisa in
- uporabljeni znaki v geslu.

Napad bomo opravljali po sledečem postopku.

Splošni postopek

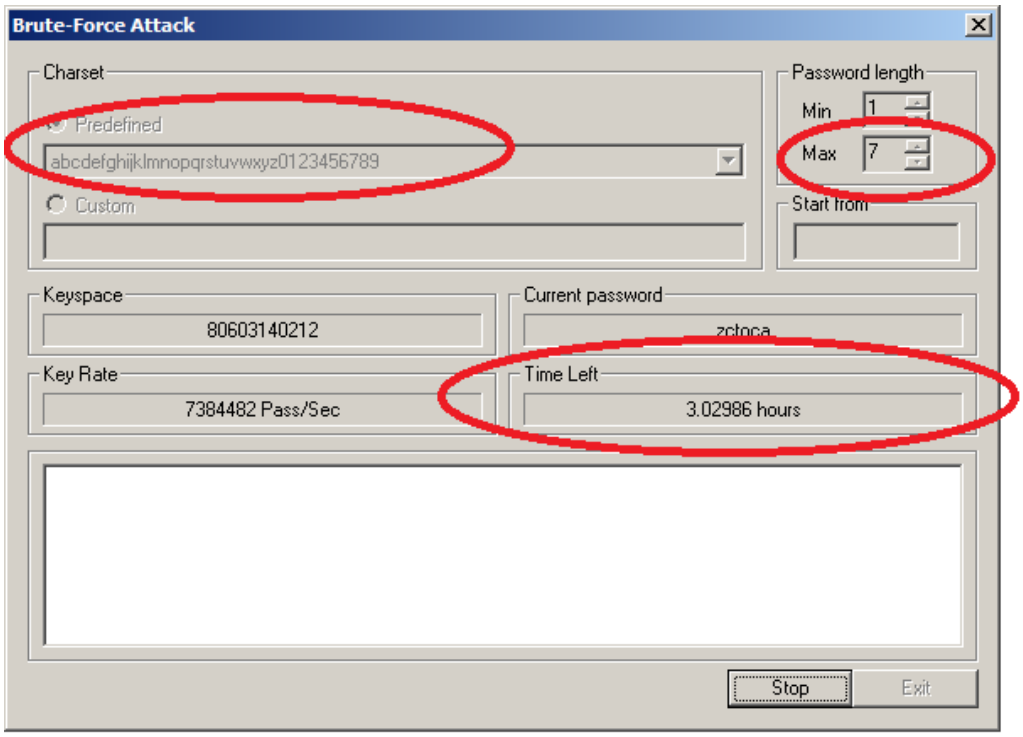
1) Izberite geslo dolžine ***N***, v katerem uporabite znake iz nabora ***Z***.
(***N*** *in* ***Z*** *sta definirana v nadaljevanju*)

2) S pomočjo HASH kalkulatorja izračunajte njihove odtise s postopki MD4, MD5, SHA-1, 256 bitnim SHA-2 in 512 bitnim SHA-2

3) Razbijalca nastavite, kot prikazuje spodnja slika.

4) Z razbijalcem poskušajte razkriti gesla, pri tem pa izmerite čas. Pri vsakem razbijanju počakajte eno minuto. Če se v tem času geslo ne razkrije, si zabeležite čas »Time Left«, ki mu prištejete preteklo minuto.

5) Rezultate vpisujte v pripravljeno tabelo.



Nalogo opravite za

- dolžine gesel ***N***={ 5, 6, 7, 10 }
- ***Z*** = geslo ki vsebuje
    - { samo črke;
    - črke in številke}

	n=5		**n=6**		**n=7**	**n=10**
	samo črke	**črke + št.**	**samo črke**	**črke + št.**	**samo črke**	**samo črke**
MD4						
MD5						
SHA-1						
SHA-2 (256 bit)						
SHA-2 (512 bit)						

Na podlagi meritev si zapišite ugotovitve.

Napad na podlagi slovarja

Splošni postopek

1) Izberite si angleško besedo z vsaj 5 črkami brez drugih znakov (npr. »million«). Bodite pozorni na pravilno črkovanje.

2) Izbrano besedo pretvorite v geslo z uporabo postopkov iz nabora ***G***, ki je definiran v nadaljevanju.

3) Z uporabo algoritmov MD5 in SHA-2 (512 bit) izračunajte odtis gesla.

4) Izvedite napad na podlagi slovarja.

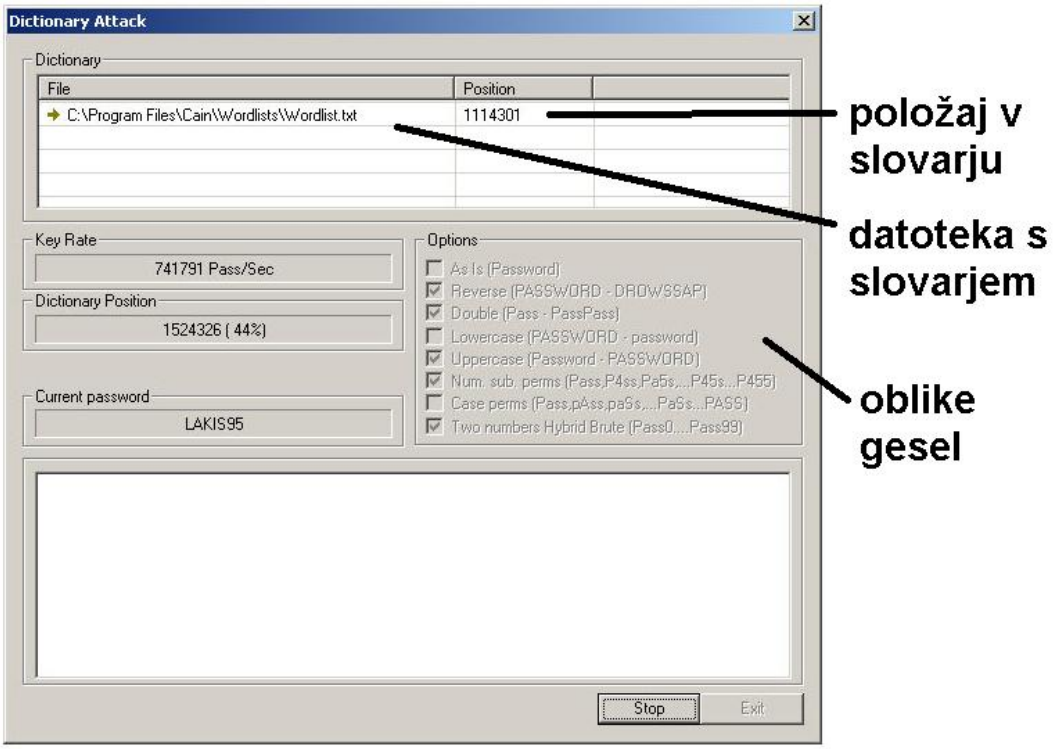
5) Pred prvim napadom morate naložiti datoteko s slovarjem.

6) Pred vsemi ostalimi napadi morate nastaviti položaj v slovarju na začetek (desni klik na datoteko s slovarjem/reset initial file position).

7) Nastavitev ***Options*** nastavite tako, da bo vedno izbrana le tista možnost, ki ustreza vaši obliki gesla. Poleg nje naj bosta izbrani le še ***Lowercase*** in ***Uppercase***.

8) Z razbijalcem poskušajte razkriti gesla, pri tem pa izmerite čas. Rezultate vpisujte v pripravljeno tabelo.

9) Primerjajte učinkovitost napada na podlagi slovarja in napada z uporabo surove sile.



Gesla tvorite iz angleške besede po sledečih postopkih.

G = { **g1 = geslo je enako kot izbrana angleška beseda (As Is)**, npr »milllion«;

g2 = geslo je izbrana beseda zapisano v obratni smeri (**Reverse**), npr. »noillim«;

g3 = geslo je dvakrat ponovljena izbrana beseda (Double), npr. »millionmillion«;

g4 = v besedi nadomestite nekatere črke s številkami (Num. sub. perms), npr. »mi11i0n«

g5 = v izbrani besedi opravite permutacijo velikih in malih črk (**Case perms**), npr. »MiLliOn«

g6 = na konec besede dodajte dve številki (Two numbers Hybrid Brute), npr. »million66«

}

	geslo	**slovar**		**surova sila**	
		MD5	**SHA-2 (512 bit)**	**MD5**	**SHA-2 (512 bit)**
g1					
g2					
g3					
g4					
g5					
g6					

Na podlagi meritev si zapišite ugotovitve.

Napad na podlagi mavričnih tabel

Splošni postopek

1) Izberite si tri netrivialna gesla, dolga 8 znakov, ki naj vsebujejo le male črke in številke.

2) Z uporabo algoritma MD5 izračunajte odtis gesel.

3) Izvedite napad na podlagi mavričnih tabel.

4) Pred prvim napadom morate naložiti datoteke z mavričnimi tabelami.

5) Z razbijalcem poskušajte razkriti geslo, pri tem pa izmerite čas. Rezultate vpisujte v pripravljeno tabelo.

6) Primerjajte učinkovitost napada na podlagi mavričnih tabel v primerjavi s postopkom uporabe surove sile.

geslo	mavrična tabela	surova sila

Na podlagi meritev si zapišite ugotovitve.

Kakšno je varno geslo?