

Laboratorinis darbas Nr.1 „Slaptažodžiai“

1. DARBO TIKSLAS.

- 1.1. Patikrinti studentų sudarytų slaptažodžių stiprumą panaudojant programą <http://www.passwordmeter.com/> (laboratorijoje) – **užduotis Nr.1**
 - 1.2. Panaudojant OS Kali Linux programų rinkinį pabandyti atspėti slaptažodį. (laboratorijoje) – **užduotis Nr.2**
 - 1.3. Išbandyti įvairius Internetu randamus slaptažodžio atspėjimo įrankius (kiekvienas studentas panaudoja skirtingą įrankį). (namie) – **užduotis Nr.3**
2. Užpildyti šioje formoje pateiktas lenteles ir išsaugoti demonstruojamo įrankio ekrano kopijas bei patalpinti adresu moodle.if.ktu.lt

3 SLAPTAŽODŽIŲ SUDARYMAS IR JŲ STIPRUMO ĮVERTINIMAS

Daugumoje autentifikavimo sistemų autentifikavimas vyksta naudojant slaptažodžius, yra svarbu suprasti, kaip geras slaptažodis padeda apsaugoti prieigą prie informacinių sistemų ir jose saugomą informaciją. Nulaužus slaptažodį, tai gali būti panaudojama informacinės sistemos sukompromitavimui. Tam gali būti panaudotos įvairios atakos, nukreiptos slaptažodžių atskleidimui. Po slaptažodžio nulaužimo paprastai seka kito tipo atakos.

Dažniausiai įsilaužėliai atspėja slaptažodžius skirdami tam pakankamai laiko ir pasinaudodami programiniais produktais. Stiprių slaptažodžių panaudojimas yra gera priemonė prieš slaptažodžių atspėjimo atakas. Tokių atakų metu yra daug laiko pastebėti įsilaužimo procesus ir apsaugoti sistemas nuo tolimesnių pažeidimų.

3.1.Patarimai kaip pasirinkti slaptažodį

- 3.1.1.Imkite eilutę iš eilėraščio, dainos, ar posakio. Naudokite po vieną kiekvieno žodžio raidę. Pavyzdžiui, Kaip gyveni – gerai. Kaip tu jauties?-laimingai! Kg?gKj?!
- 3.1.2. Pasinaudokite atsitiktinių slaptažodžių generatoriumi ir pasirinkite tokią seką, kurią būtų lengva įsiminti, pavyzdžiui seka ategr04 ją galima įsiminti kaip Atėnai-Graikija 2004 –ir įdėjus didžiąsias raides ategr!4 turėsim slaptažodį.
- 3.1.3. Naudokite du paprastus žodžius, sujungtus koku nors ženklu, pavyzdžiui As&Tu?=m ar dar kažkaip panašiai.
- 3.1.4. Pakeiskite skaičiais kai kurias raides ir gaukite pakankamai paprastą slaptažodį, pavyzdžiui, 1H8work!

Taisyklės, taikomos tradiciniams slaptažodžiams:

TAIKYTINA	NENAUDOTI
Slaptažodyje naudokite tiek mažąsias tiek didžiąsias raides. Naudokite didžiąsias raides keliose vietose slaptažodyje.	Nenaudokite prisijungimo prie tinklo login ID kaip slaptažodį bet kokioje formoje (nei atvirkščia tvarka, nei didžiosiom raidėm, ar kartojant raides).
Naudokite slaptažodžius, kuriuose yra tiek raidiniai tiek skaitmeniniai simboliai, operacinės sistemos palaikomi skyrybos ženklai.	Nenaudokite savo vardo, pavardės ar kažko panašaus. Nenaudokite savo inicialų ar savų “nick” vardų ar panašiai.
Naudokite tiek didžiąsias, tiek mažąsias raides.	Nenaudokite vardų, kurie yra anglų ar kitos kalbos žodyne ar rašybos tikrinimo saraše, nenaudokite ir trumpinių.
Neįpraskite tik pradėti slaptažodį iš didžiosios raidės – naudokite didžiąsias raides ir kitose vietose.	Nenaudokite jokios kitos lengvai apie jus sužinomos informacijos (gatvės pav.,tel NR., automobilio markės ir t.t.)
Naudokite nemažiau šešių-aštuonių simbolių	Nenaudokite slaptažodžio sudaryto vien iš skaičių ar
Naudokite atsitiktinę iš pažiūros skaičių-raidžių seką.	

Naudokite slaptažodį, kurį galėtumėte lengvai įvesti, nežiūrėdami į klaviatūrą. Tai padės apsisaugoti nuo slaptažodžio atspėjimo stebint per petį.

Reguliariai keiskite slaptažodžius. Kuo kritiškesnei sistemos daliai naudojamas tas slaptažodis tuo dažniau reiktų jį keisti. Tai leis sustabdyti tuos, kurie gal būt jau spėjo sužinoti jūsų slaptažodį.

vien vien iš alfabeto raidžių. Maišykite skaičius su raidėmis.

Nenaudokite datų, pavyzdžiui Rugs2004 ar panašių kombinacijų.

Nenaudokite greta einančių klavišų sekos, pavyzdžiui, qwerty.

Nenaudokite pavyzdinio slaptažodžio gauto iš knygų ar kitokių priemonių apie saugą, nesvarbu koks stiprus jis bebūtų

Nenaudokite bet kokių iš aukščiau paminėtų žodžių, užrašytų atvirkščia tvarka ar didžiosiom raidėm ar kita kokia lengvai atspėjama forma.

Neužsirašinėkite slaptažodžių ant lipdukų, kalendorių, nesaugokite jų kompiuteryje, kur jis gali būti kitų pasiekiamas.

Nesinaudokite bendrai dalijamais prisijungimais.

Sunku vesti apskaitą bei nusakyti atsakomybę esant grupiniam naudojimui

Niekam neatskleiskite savo slaptažodžio.

4. UŽDUOTIS NR.1

Sugalvokite paprastą slaptažodį (naudodami tik mažąsias raides). Pasinaudodami nuoroda <http://www.passwordmeter.com/> patikrinkite to slaptažodžio stiprumą. Taip pat patikrinkite dar dviejų sudėtingesnių slaptažodžių stiprumą. Rezultatus surašykite į lentelę.

1 lentelė. Slaptažodžių stiprumo nustatymo rezultatai panaudojant <http://www.passwordmeter.com/>

Slaptažodžio stiprumas	Sugalvotas slaptažodis	Realus stiprumas
Silpnas < 50%	123	4%
Stipresnis < 100%	Jhon567	56%
Stiprus = 100%	Spider...123	100%

Dėmesio!!! Niekada nenaudokite tokių (jūsų nevaldomų) sistemų savo tikrų slaptažodžių patikrinimui.

5. UŽDUOTIS NR. 2. SLAPTAŽODŽIŲ ATSPĖJIMAS PANAUDOJANT OS KALI LINUX PROGRAMŲ RINKINĮ

ISO atvaizdą galima parsisiųsti iš: <https://www.kali.org/downloads/> ir atsidarykite jį savo kompiuteryje naudodami virtualią aplinką pvz., VMware player.

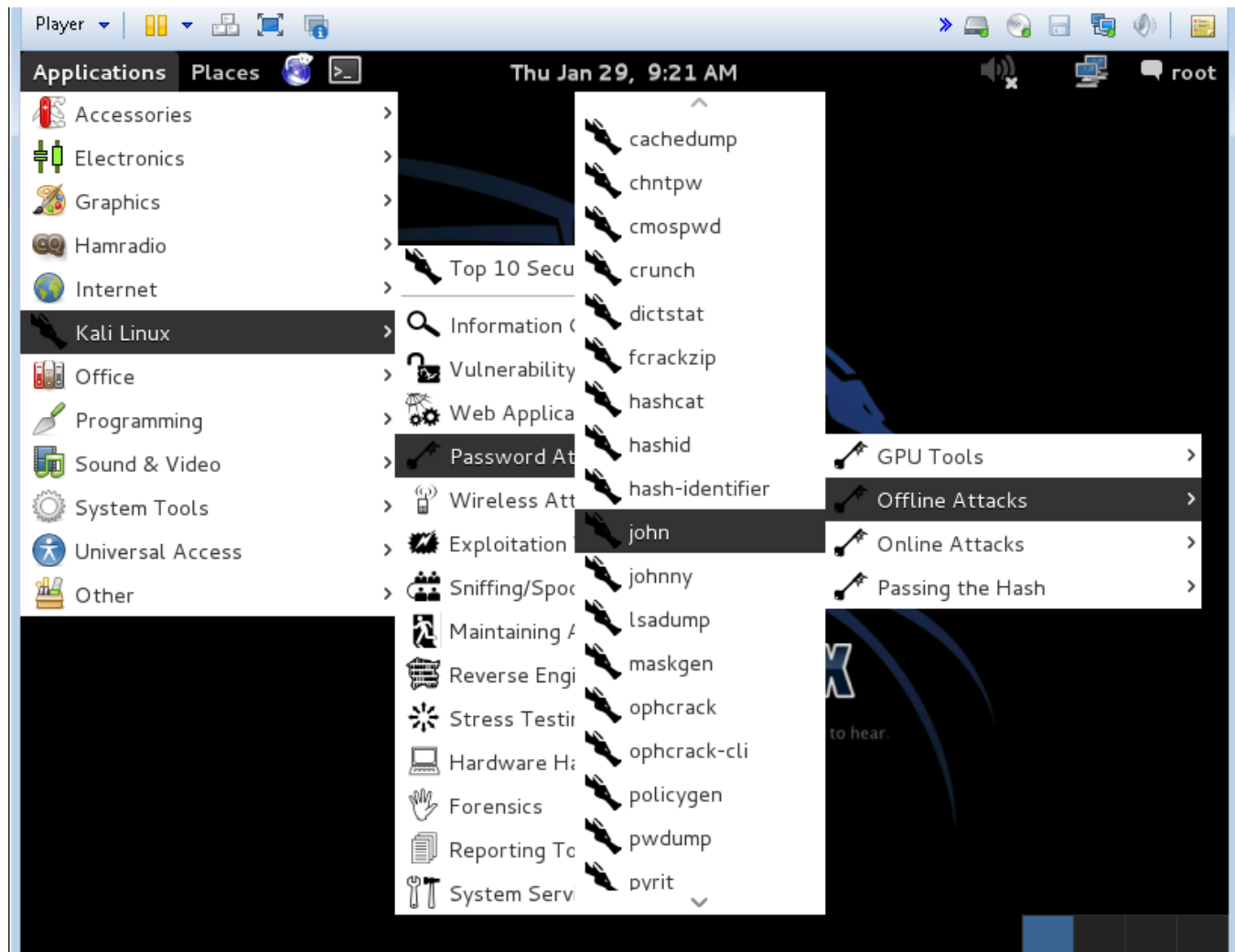
Slaptažodžio atsėjimui naudokite įrankį: **Applications/05-Passaword Attacks/John**

Norint sužinoti vartotojų slaptažodžius galima pasinaudoti John the Ripper įrankiu:

Panaudojant OS Kali Linux programų rinkinį

<https://www.blackmoreops.com/2015/11/10/cracking-password-in-kali-linux-using-john-the-ripper/>

Ankstesnis rinkinys panaudojamas kaip nurodyta paveiksle:



John the Ripper įrankio įjungimo nuoroda

Taip pat galima parsisiųsti iš : <http://www.openwall.com/john/>

Jeigu naudojama versija:

`Kali-Linux-2016.2-vbox-amd64`

`Debian (64-bit)`

tada reikiamas įrankis surandamas adresu:

`Applications/05-Password Attacks/john`

Tolimesniuose žingsniuose nurodytuose nuo 5.1. iki 5.8, įvykdytų komandų tekstą atspausdinkite.

Užduoties Nr.2 atlikimo eiga

5.1. Sukuriame naują vartotoją:

`#adduser vartotojas`

5.2. Vartotojui sukuriame lengva **slaptažodį** pvz. *“demo”*, kitus vartotojo duomenis palikti tuščius.

5.3. Pareiname į sukurto vartotojo failų direktoriją.

```
#cd /home/vartotojas
```

5.4. Nukopijuokime failus *passwd* ir *shadow* į */home/vartotojas* katalogą:

```
#cp /etc/passwd /etc/shadow /home/vartotojas
```

5.5. Patikriname ar failai nusikopijavo ir yra kataloge.

```
#ls
```

Toliau atliksime vartotojų slaptažodžių šifravimą /home/vartotojas direktorijoje.

5.6. Paleidžiame *unshadow* komandą :

```
#unshadow passwd shadow > crack_mano.txt
```

5.7. Paleidžiame slaptažodžio atspėjimo programą John The Ripper :

```
#./john crack_mano.txt
```

Ekrane pamatome vartotojų prisijungimo duomenis.

5.8. Antra kartą norint pasižiūrėti slaptažodį reikia paleisti šią komandą:

```
#john --show crack_mano.txt
```

6. NAMŲ UŽDUOTIS Nr.3 DARBO ATSISKAITYMUI

6.1. Moodle sistemoje yra įrankių paskirstymas studentams. Jei dėl kokių nors priežasčių jums paskirtas įrankis nedarba, **nurodykite priežastį** ir pasirinkite naują įrankį. Naujas įrankis turi nesutapti nei su vienu studentams paskirtu įrankiu.

6.2. Trumpai aprašant įrankio išbandymą reikalingos ekrano kopijos (printscreens), kuriose su raudona rodykle pažymimi tik ypatingi punktai, su lakonišku aprašymu kas buvo daryta ir parašymu ką spausti, kad atlikti reikalingus veiksmus. Ekrano kopijos paliekamos anglų kalba.

6.3. Sugalvokite ne mažiau tris slaptažodžius su įvairiais stiprumo lygiais ir užpildykite lentelę.

Nedas Liaudanskis IFF-1/9

MD5 brutforce.py

Veikimo principas:

Parsisūsti repositoryją iš <https://github.com/sefasaid/python-md5-bruteforce>

- Atsidaryti komandinį langą.
- Nueiti į repositoryjos direktoriją.
- Paleidimui naudoti šią komandą: \$ python2 md5-bruteforce.py
- Atsiradus tekstui add md5, tiesiog įdėti md5 hash slaptažodį.

Įrankis naudoja bruteforce metodą surasti užšifruotą slaptažodį. Naudojant šį metodą atšifruoti slaptažodį užtrunka ilgai, priklausomai nuo slaptažodžio dydžio. Nes yra bandomos įvairios kombinacijos. Bandžiau naudoti šiam namų darbui ir wordlist metodą. Šis metodas labai greitas, tačiau neturint tinkamai paruošto failo su žodžių rinkiniu, daugumą ieškotų slaptažodžių, buvo tiesiog nesurasti.

Pirmas Bandymas:


Slaptažodis: 123456789

Iššifravimo laikas: >3600 sek.

```
(kali㉿kali)-[~/Desktop/python-md5-bruteforce]
$ python2 md5-bruteforce.py
```

```
Name           : Python Md5 Brute-force
Created By      : Sefa Said Deniz
Blog           : sefasaiddeniz.com
Documentation   : https://github.com/sefasaid/python-md5-bruteforce/
License        : Completely Free
Thanks to      : Agus Makmun (Summon Agus)-bloggersmart.net - pyth
on.web.id
```

```
add md5
25f9e794323b453885f5181f1b624d0b
0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ!"#$%&'(
)*+,-./:;=<=>?@[\]^_`{|}~
[+] Start Time: 03:05:16
```



```
kali@kali: ~/Desktop/python-md5-bruteforce
File Actions Edit View Help
add md5
25f9e794323b453885f5181f1b624d0b
0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ!"#$%&'(
)*+,-./:;=<=>?@[\]^_`{|}~
[+] Start Time: 03:05:16
loading |
[!] I'm at 1 -character

[!] 1 -character finished in 0.000320911407471 seconds —

[!] I'm at 2 -character

[!] 2 -character finished in 0.00501203536987 seconds —

[!] I'm at 3 -character
loading |
[!] 3 -character finished in 0.452027082443 seconds —

[!] I'm at 4 -character
loading |
[!] 4 -character finished in 44.2029139996 seconds —

[!] I'm at 5 -character
loading \█
```

MD5 Hash Generator

Use this generator to create an MD5 hash of a string:

123456789

Generate →

Your String	123456789
MD5 Hash	25f9e794323b453885f5181f1b624d0b

Copy

Antras Bandymas:

Slaptažodis: 123

Iššifravimo laikas: 10 sek.

MD5 Hash Generator

Use this generator to create an MD5 hash of a string:

123

Generate →

Your String	123
MD5 Hash	202cb962ac59075b964b07152d234b70 <button>Copy</button>
SHA1 Hash	40bd001563085fc35165329ea1ff5c5ecbdbbfeef <button>Copy</button>

```
kali@kali: ~/Desktop/python-md5-bruteforce
File Actions Edit View Help

add md5
202cb962ac59075b964b07152d234b70
0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ!#$%&'()*+,-
./:;<=>?@[\]^_`{|}~
[+] Start Time: 04:21:31
loading |
[!] I'm at 1 -character

[!] 1 -character finished in 0.000140190124512 seconds —
[!] I'm at 2 -character

[!] 2 -character finished in 0.00486493110657 seconds —
[!] I'm at 3 -character
loading -
[!] found 123

[-] End Time: 04:21:41
[-] Total Keyword attempted: 17958

—Md5 cracked at 10.0206229687 seconds —
```


Trečias Bandydas:

Slaptažodis: Jhon5

Iššifravimo laikas: 2426 sek.

MD5 Hash Generator

Use this generator to create an MD5 hash of a string:

Jhon5

Generate →

Your String	Jhon5
MD5 Hash	7c610c2ffc2fa7476a7d8044923ef6b8 <button>Copy</button>
SHA1 Hash	1f68ca46d39143036cd26ba9e4867a73b93d0655 <button>Copy</button>

```
kali@kali: ~/Desktop/python-md5-bruteforce
File Actions Edit View Help

[!] 2 -character finished in 0.00646305084229 seconds —
[!] I'm at 3 -character
loading /
[!] 3 -character finished in 0.5239341259 seconds —
[!] I'm at 4 -character
loading -
loading \ 4 -character finished in 49.8657810688 seconds —
[!] I'm at 5 -character
loading |
[!] found Jhon5

[-] End Time: 05:03:53
[-] Total Keyword attempted: 3606618890

—Md5 cracked at 2426.20507097 seconds —
Thank You !
```


Sugalvotų slaptažodžių įveikimo parametrų lentelė:

Slaptažodžio įveikimo laikas (sek.)	Sugalvotas slaptažodis	Realus stiprumas
10 sek.	123	Labai silpnas
2426 sek.	Jhon5	Silpnas
Daugiau nei 3600 sek.	123456789	Labai silpnas

7. Darbo vertinimo kriterijai

Lab. darbas vertinamas, kai moodle yra išsaugoti ir parengti 2 failai:

1) klasėje A, B užduotys lab. task report "Pasword cracking and strengthevaluation" "Word"-ataskaita laboratorinio metu.

2a) namuose, kai atsiskaitymui demonstruojamas įrankis gyvai per projektorį, tuomet iš ekrano kopijų sukuriamas "Word" failas-galutinė ataskaita (gynimas maks. 10 balams, jeigu įrankis neatlieka slaptažodžio nulaužimo maks. 8 balai).

ARBA

2b) namuose, kai atsiskaitymui demonstruojamas "ppt" pateiktys, tuomet iš ekrano kopijų sukuriamas "PowerPoint" failas-galutinė ataskaita (gynimas maks. 8 balams, jeigu įrankis neatlieka slaptažodžio nulaužimo maks. 6 balai).