



Zaštita računarskih sistema i mreža

- Sedma laboratorijska vežba -

7. Windows lozinke, Rainbow tabele, podrazumevane lozinke¹

Na Windows računarima postoji SAM-Security Account Manager fajl koji predstavlja bazu podataka gde se čuvaju lozinke i ostali korisnički podaci za taj računar. Za vreme rada računara SAM fajl je zaključan i ne može da mu pristupi i da ga izmeni bilo koji proces, ali je učitao u jedan deo RAM memorije kome može da se pristupi sa administratorskim privilegijama. Windows ne koristi salt za čuvanje svojih lozinki kao linux već ih čuva enkriptovane u formatu `Username:UserID:LMHash:NTLMHash::::`. Biće ilustrovano kako uz pomoć nekih alata doći do SAM fajla, kako se generišu rainbow tabele koje imaju veliki uticaj u brzini razbijanja lozinki i na primeru će biti prikazano kako rainbow tabele pomažu u razbijanju lozinki.

Na Windows 7 virtuelnoj mašini sa administratorskim pristupom potrebno je kreirati druge korisnike i posmatrati koliko Rainbow tabele pomažu u razbijanju lozinki. U realnoj situaciji računar na kom se vrši dohvaćanje SAM fajla i računar na kome se vrši razbijanje lozinki ne bi bili isti, ali za potrebe demonstracije se koristi isti računar.

Na desktopu virtuelne mašine VM2 se nalaze dva foldera potrebna za izradu ove mreže:

- Lab 7 tools u kojem se nalaze alati koji će se koristiti za izradu ove vežbe (u ovom folderu ima više alata od onoga što je prikazano u ovoj lab vežbi. Savetuje se studentima da probaju samostalno da isprobaju i ostale alate koji su u tom folderu – posebno alate za steganografiju slika i whitespace alat za steganografiju snow)
- Lab 7 tables u kojem se nalaze rainbow tabele lozinki preuzete sa sledećeg [linka](#). Preuzete su tabele Vista free (461MB) i Vista proba free (581MB), a pogledati koje sve tabele još postoje.

7.1 Pwdump7-Ilustracija rada alata pwdump

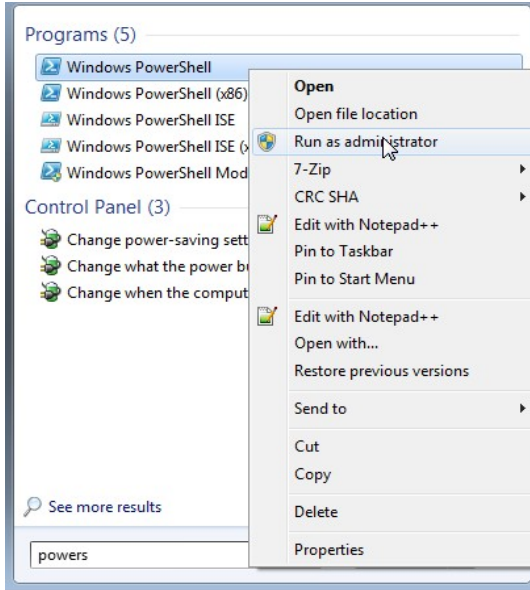
Alati pwdump (Password dump) se koriste za dohvaćanje SAM fajla Windows računara na kom korisnik ima pristup i kontrolu. Ovi alati zahtevaju administrativna prava i novije verzije Windows-a i pretraživača ih prepoznaju kao viruse i preteći softver, pa se iz tog razloga za njihovu upotrebu moraju deaktivirati antivirus ili Windows Defender. Njihova alternativa su alati koji SAM fajl dohvataju sa hard diska na kome je instaliran Windows operativni sistem, ali nije podignut.

1. Pokušati otvaranje SAM fajla na lokaciji "C:\Windows\System32\config\SAM" korišćenjem notepad-a i dvoklikom na fajl. Primetiti da su za pristup ovoj lokaciji potrebna ad-

¹ Nastavnici na predmetu Zaštita računarskih sistema i mreža se zahvaljuju studentu Luki Mrdaku za pripremu scenarija ovu laboratorijsku vežbu

ministratorska prava. Primetiti prilikom otvaranja foldera u kom se nalazi SAM fajl da se pored njega nalazi ključ, što znači da je fajl zaključan. Primetiti da se prilikom otvaranja SAM fajla korišćenjem notepad-a otvara prazan fajl i prikazuje greška.

2. Sada je potrebno doći do sadržaja SAM fajla korišćenjem alata Pwdump7. To je alat bez GUI-ja, pa je njegovo pokretanje potrebno koristiti PowerShell ili komandni interfejs. U ovoj lab vežbi je prikazano korišćenje PowerShell-a. Pritisnuti Start i otkucati PowerShell. Pokrenuti program kao administrator. Potvrditi izbor klikom na yes.



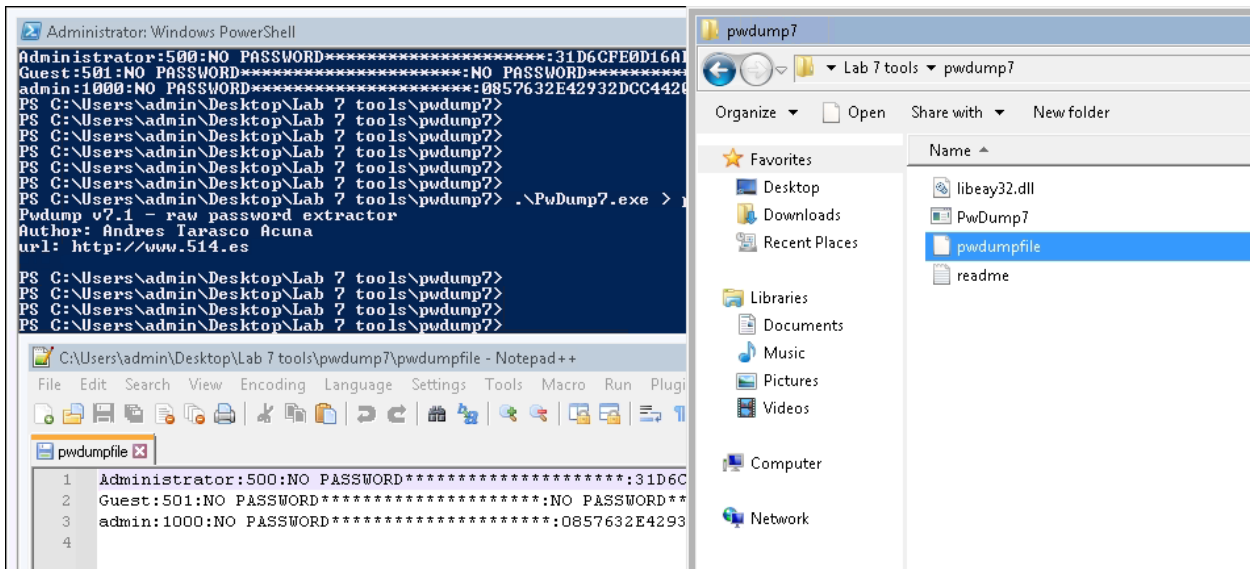
3. Potrebno je pozicionirati se unutar direktorijuma gde se nalazi program Pwdump. Komanda za prelazak u neki direktorijum je **cd ime_direktorijuma**. Komanda za povratak direktorijum iznad je **cd ..**, a nazive direktorijuma nije potrebno kucati cele već je dovoljno prvih nekoliko slova naziva direktorijuma, a ostatak će autocomplete popuniti pritiskom na tab. Izlistavanje sadržaja tekućeg direktorijuma vrši se komandom **ls**, a konzola se čisti komandom clear.
4. Izvršiti komandu **cd C:\Users\admin\Desktop\Lab 7 tools\pwdump7**
5. Pokrenuti komandu **.\PwDump7.exe** i primetiti da se tada dump SAM fajla dobija u konzoli što je pogodno za ilustraciju, ali nema neku veliku praktičnu primenu.

```
PS C:\Users\admin\Desktop\Lab 7 tools\pwdump7> .\PwDump7.exe
PwDump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

Administrator:500:NO PASSWORD*****:31D6CFE0D16AE931B73C59D7E0C089C0:::
Guest:501:NO PASSWORD*****:NO PASSWORD*****:::
admin:1000:NO PASSWORD*****:0857632E42932DCC44201A8EA05DD8D9:::
PS C:\Users\admin\Desktop\Lab 7 tools\pwdump7>
```

6. Izlaz ove komande snimiti u fajl korišćenjem komande **.\PwDump7.exe > pwdumpfile**, gde je pwdumpfile naziv fajla u koji se snima. Tada se na konzoli ne ispisuje sadržaj SAM fajla, ali se u folderu gde se nalazi alat kreira fajl sa ovim izlazom (moguće zadati i drugu putanju).

² Uneti odgovarajuću putanju koja odgovara stvarnoj putanji na Windows mašini



Ovim je kreiran fajl sa heševima po formatu iz uvoda iz kog se jednostavno mogu dobiti lozinke korisnika što biti ilustrirano u narednom delu lab vežbe.

Ne zatvarati Powershell jer će biti potreban kasnije

7.2 Winrtgen-Primer generisanja rainbow tabele

U folderu Lab 7 tools koji je smešten na Desktopu nalaze se alati za generisanje rainbow tabele. Ovde će na primeru biti ilustrirano koliko vremena je potrebno za generisanje rainbow tabele i koje vreme one štede prilikom razbijanja lozinke.

1. Otvoriti folder Lab 7 tools, pa unutar njega pronaći folder Winrtgen. Korišćenjem tog alata će biti demonstrirano kreiranje rainbow tabele.
2. Otvoriti fajl charset u Notepad++. Primetiti razne alfabete i to da neki od njih koriste isključivo mala ili isključivo velika slova (case-sensitive i case-insensitive lozinke), brojeve i lokalne karaktere. Što je veći alfabet to izračunavanje rainbow tabele duže traje.

```
numeric = {0123456789}
numeric-space = {0123456789 }
loweralpha-DG = {abcdefghijklmnopqrstuvwxyzæåäöüß}
loweralpha-space-DG = {abcdefghijklmnopqrstuvwxyzæåäöüß }
loweralpha-num-DG = {abcdefghijklmnopqrstuvwxyz0123456789æåäöüß}
loweralpha-num-space-DG = {abcdefghijklmnopqrstuvwxyz0123456789æåäöüß }
loweralpha-num-symbol14-DG = {abcdefghijklmnopqrstuvwxyzäöüß0123456789!@#$%^&*()-_+=~'[]{}|\\:;'"<>./?/æåäöüß}
loweralpha-num-all-DG = {abcdefghijklmnopqrstuvwxyzäöüß0123456789!@#$%^&*()-_+=~'[]{}|\\:;'"<>./?/æåäöüß}
loweralpha-num-all-space-DG = {abcdefghijklmnopqrstuvwxyzäöüß0123456789!@#$%^&*()-_+=~'[]{}|\\:;'"<>./?/æåäöüß }

mixalpha-DG = {abcdefghijklmnopqrstuvwxyzæåäöüßABCDEFGHIJKLMNopqrstuvwxyzÆÖÄÖÜ}
mixalpha-space-DG = {abcdefghijklmnopqrstuvwxyzæåäöüßABCDEFGHIJKLMNopqrstuvwxyzÆÖÄÖÜ }
mixalpha-num-DG = {abcdefghijklmnopqrstuvwxyzæåäöüßABCDEFGHIJKLMNopqrstuvwxyz0123456789ÆÖÄÖÜ}
mixalpha-num-space-DG = {abcdefghijklmnopqrstuvwxyzæåäöüßABCDEFGHIJKLMNopqrstuvwxyz0123456789ÆÖÄÖÜ }
mixalpha-num-symbol14-DG = {abcdefghijklmnopqrstuvwxyzæåäöüßABCDEFGHIJKLMNopqrstuvwxyz0123456789!@#$%^&*()-_+=~'[]{}|\\:;'"<>./?/æåäöüß}
mixalpha-num-all-DG = {abcdefghijklmnopqrstuvwxyzæåäöüßABCDEFGHIJKLMNopqrstuvwxyz0123456789!@#$%^&*()-_+=~'[]{}|\\:;'"<>./?/æåäöüß}
mixalpha-num-all-space-DG = {abcdefghijklmnopqrstuvwxyzæåäöüßABCDEFGHIJKLMNopqrstuvwxyz0123456789!@#$%^&*()-_+=~'[]{}|\\:;'"<>./?/æåäöüß }
```

3. Otvoriti program Winrtgen. Pritisnuti na dugme Add Table.

Rainbow Table properties

Hash: Min Len: Max Len: Index: Chain Len: Chain Count: N° of tables:

Charset: Edit

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Table properties

Key space: 8353082582 keys
Disk space: 610.35 MB
Success probability: 0.978038 (97.80%)

Benchmark:

Hash speed:
Step speed:
Table precomputation time:
Total precomputation time:
Max cryptanalysis time:

Optional parameter:

Benchmark OK Cancel

Objašnjenje parametara za generisanje jedne rainbow tabele

Pojam	Značenje
Hash	Koji algoritam za heširanje će se koristiti. To mogu biti na primer lm (Win XP), ntlm (Win 7), wpa-psk (WiFi), sha512, sha1, md5 itd.
Min/Max Len	Minimalna i maksimalna dužina lozinke za koju će se kreirati heševi
Charset	Alfabet od kojeg će se računati heševi
Index	Diskriminator tabela. Moguće je da se jedna tabela zbog veličine nalazi u više fajlova, a oni fajlovi koji imaju isti indeks predstavljaju istu tabelu

Klikom na dugme Benchmark vrši se provera koliko heševa u sekundi računar može izračunati i koliko bi mu vremena bilo potrebno za računanje zadatog posla. Veliko ubrzanje može se ostvariti dodavanjem grafičkih kartica koje imaju mnogo paralelnih procesora, takozvanih CUDA jezgara. Razmisliti o tome koliko bi vremena bilo potrebno za razbijanje lozinke kada ne bi imali rainbow tabele već kada bi sve heševe iznova svaki put računali.

Kliknuti na OK, a zatim na Start i posmatrati kako se odvija proces pravljenja hash-eva. Prekinite proces posle nekog vremena jer može da potraje i da prepuni disk virtuelne mašine. Ovo je samo demonstracija rada alata za generisanje rainbow tabela hash-eva.

Rainbow Table properties

Hash: Min Len: Max Len: Index: Chain Len: Chain Count: N° of tables:

Charset: Edit

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Table properties

Key space: 8353082582 keys
Disk space: 610.35 MB
Success probability: 0.978038 (97.80%)

Benchmark:

Hash speed: 2863688 hash/sec
Step speed: 2236135 step/sec
Table precomputation time: 11.9253 hours
Total precomputation time: 11.9253 hours
Max cryptanalysis time: 1.28794 seconds

Optional parameter:

Benchmark OK Cancel

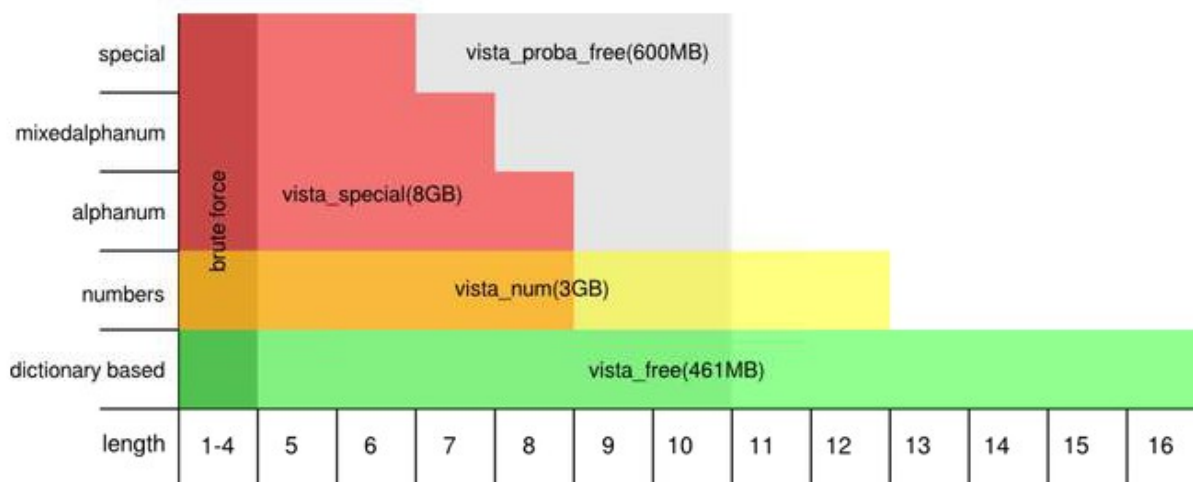
7.3 Ophcrack³-Korišćenje rainbow tabela za razbijanje lozinki

Rainbow tabele su unapred izračunate tabele izlaza kriptografskih heš funkcija. U osnovi, umesto da svaki put kada je potreban izlaz neke kriptografske heš funkcije taj izlaz računa ta vrednost se traži unutar rainbow tabele, koja se poželjno nalazi u RAM memoriji zarad bržeg pristupa. Zbog ove osobine da se rainbow tabele učitavaju u RAM memoriju one se prave iz delova, tako da jedan deo tabele nikad nije veći od 2GB.

Na slici ispod je prikazano za koje lozinke se mogu koristiti tabele hasheva sa Ophcrack sajta. U okviru foldera Lab 7 tables se nalaze vista_proba_free i vista_free tabele kojima se pronalaze kraće i jednostavnije lozinke. Za neke složenije lozinke je potrebno učitati druge tabele, ali molimo studente da to ne rade u okviru laboratorijske VM2 jer nema dovoljno resursa. Sa druge strane studenti se ohrabruju da probaju ovo na svojim računarima ako imaju dovoljno hardverskih resursa.

Free Vista Rainbow tables

These tables can be used to crack Windows Vista and 7 passwords (NT hashes).

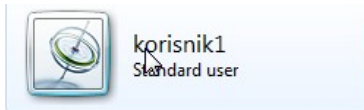


Sledeći primer ilustruje korišćenje brute force algoritma za razbijanje kratkih lozinki i upotrebu rainbow tabela za razbijanje dužih. Rainbow tabele koje će biti korišćene su *vista_free* i *vista_proba*. Vista free je bazirana na rečniku od 64 hiljade reči, 4 hiljade sufiksa, 64 prefiksa sa 4 pravila alteracije, a vista proba free je 2^{39} lozinki prema najkorišćenijim obrascima (Ime1234, ImePrezime, ImePrezime321...) i najčešćim kombinacijama karaktera unutar obrazaca. Vista proba free je trenirana na najpoznatijoj listi uobičajenih lozinki rockyou koju možete preuzeti na ovom [linku](#). Pogledati koje se lozinke nalaze na ovoj listi.

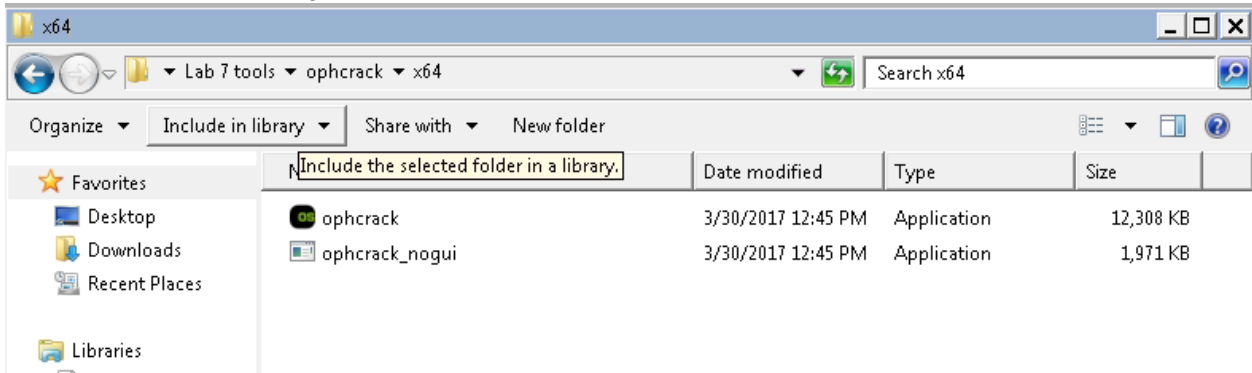
1. Otvoriti Control Panel, pa unutar njega User Accounts.
2. Kliknuti na Manage Another Account čime se otvara upravljanje ostalim nalogima.

³ Ophcrack je alat razvijen od strane Objectif Sécurité, vodeće švajcarske konsultantske kompanije u oblasti zaštite sistema. Uz svoj alat oni su kreirali rainbow tabele koje se mogu besplatno preuzeti, a na njihovom [sajtu](#) postoji i internet verzija alata ophcrack. Do decembra 2019 neke od njihovih većih rainbow tabela (2,3Tb ukupne veličine) su bile namenjene za profesionalnu upotrebu i prodavali su ih za razliku od manjih koje su uvek bile besplatne i u svom nazivu su imale reč free. Sada su sve njihove tabele besplatne i mogu se preuzeti kao torrent ili kao obično preuzimanje. Na njihovom sajtu se može pronaći i grafik za koje lozinke se mogu koristiti profesionalne tabele.

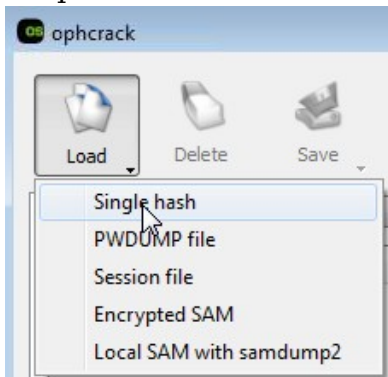
- Kliknuti na Create a new account, postaviti ime **korisnik1** (nije bitno da li je standardni korisnik ili administrator). Kliknuti na korisnika korisnik1.



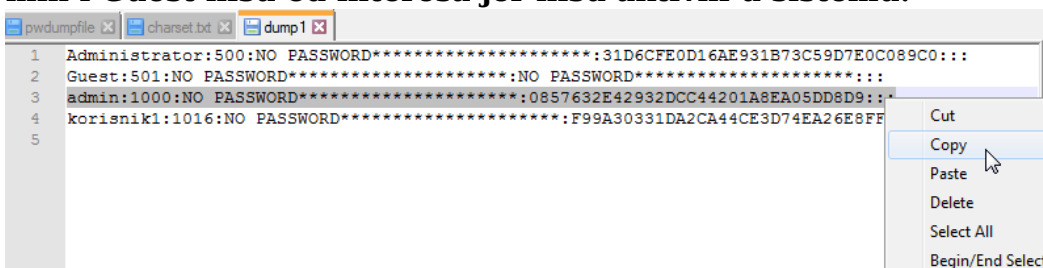
- Kliknuti na Create a password i tu postavite lozinku **aesr**
- Otvoriti ophcrack koji se nalazi na desktopu u folderu Lab 7 tools, pa ophcrack, pa x64



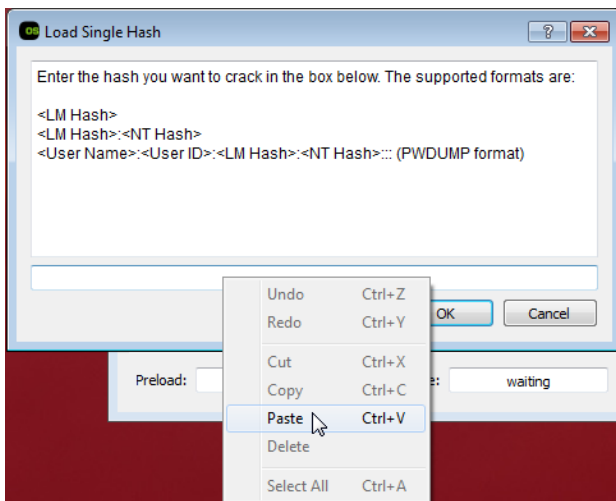
- Pratiti uputstvo za alat [PwDump7](#) i napraviti novi dump SAM fajla sa imenom dump1. Komanda za to je **.\PwDump7.exe > dump1**. Otvoriti taj fajl u notepad-u. **I dalje ne zatvarati Powershell**
- U ophcrack-u kliknuti na Load, pa single hash.



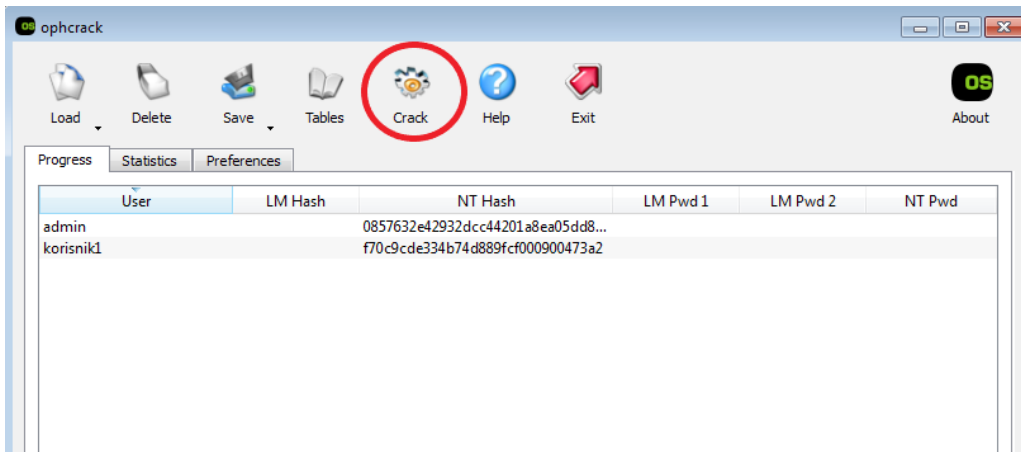
- Selektovati pojedinačni red za jednog korisnika i kopirati ga (Ctrl+C). **Korisnici Admin i Guest nisu od interesa jer nisu aktivni u sistemu.**



- Selektovani red nalepiti(Ctrl+V). Pritisnuti ok.

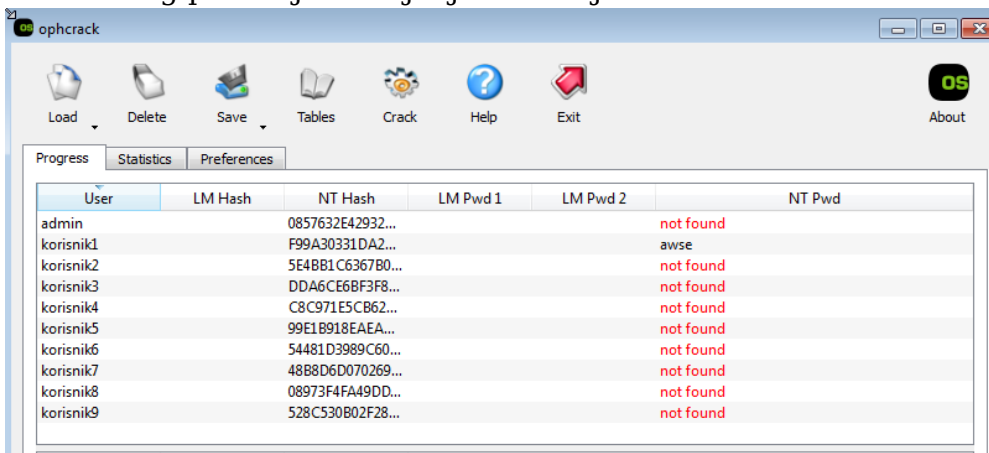


10. Korake **8** i **9** ponoviti za sve korisnike u sistemu.
11. Ukoliko postoje redovi čija kolona user počinje sa ***disabled***. Selektovati taj red i pritisnuti delete na tastaturi da biste uklonili taj red. Na ovaj način je izvršeno uklanjanje neaktivnih korisničkih naloga koji bi samo usporavali razbijanje lozinki.
12. Nakon što su uvezeni heševi korisničkih naloga potrebno je pokrenuti razbijanje lozinki klikom na Crack dugme. Očekivano vreme ovog pokušaja razbijanja lozinki je oko deset sekundi.

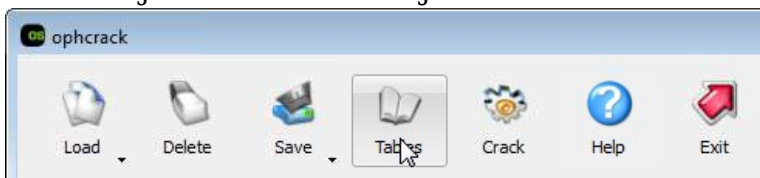


13. U koloni NT Pwd primetiti da je za korisnika korisnik1 pronađena lozinka i to korišćenjem samo brute force algoritma. Pogledati grafik iznad i primetiti da je za lozinke dužine do 4 karaktera dovoljan brute force algoritam za njihovo razbijanje bez ikakvih rainbow tabela.
14. Ponoviti korake od 2 do 6 i kreirati korisnika sa imenom **korisnik2** sa lozinkom **barney**
15. Ponoviti korake od 2 do 6 i kreirati korisnika sa imenom **korisnik3** sa lozinkom **barney1234**
16. Ponoviti korake od 2 do 6 i kreirati korisnika sa imenom **korisnik4** sa lozinkom **stinson**
17. Ponoviti korake od 2 do 6 i kreirati korisnika sa imenom **korisnik5** sa lozinkom **stinson321**
18. Ponoviti korake od 2 do 6 i kreirati korisnika sa imenom **korisnik6** sa lozinkom **917790540**
19. Ponoviti korake od 2 do 6 i kreirati korisnika sa imenom **korisnik7** sa lozinkom **1122334455**

20. Ponoviti korake od 2 do 6 i kreirati korisnika sa imenom **korisnik8** sa lozinkom **1122334455a**
21. Ponoviti korake od 2 do 6 i kreirati korisnika sa imenom **korisnik9** sa lozinkom **! Class1cs!**
22. Pratiti uputstvo za alat [PwDump7](#) i napraviti dump SAM fajla sa imenom dump2. (Poslednja komanda iz istorije se učitava pritiskom na strelicu naviše) Komanda za to je **.PwDump7.exe > dump2**. Otvoriti taj fajl u notepad-u. Zatvoriti Powershell.
23. Otvoriti ophcrack i ponoviti korake **8** i **9** i ubaciti sve korisnike od korisnik1 do korisnik9 i admin.
24. Klikom na Crack pokrenuti razbijanje lozinki, ali ovaj put sa manje uspeha. Očekivano vreme ovog pokušaja razbijanja lozinki je oko deset sekundi.



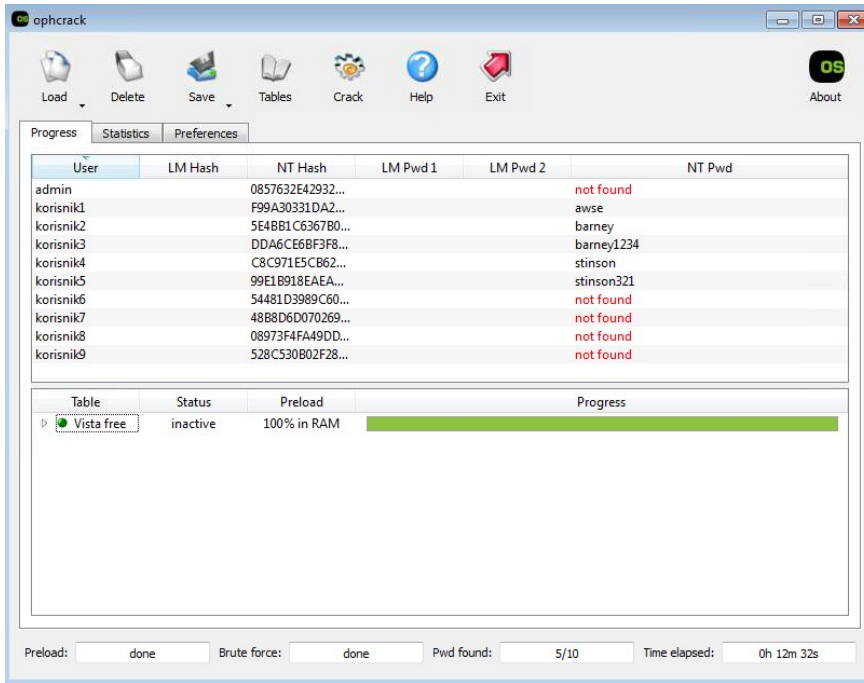
25. Sada je potrebno učitati rainbow tabele koje ubrzati razbijanje lozinki. Pritisnuti dugme tables koje služi za dodavanje rainbow tabela.



26. Pritisnuti dugme install i pokazati na folder na desktopu gde je na početku laboratorijske vežbe otpakovana tabela vista free. Kliknuti na ok.

XP german v2		not installed	on disk
Vista special		not installed	on disk
Vista free	C:\Users\admin\Desktop\tables_vista_free	inactive	on disk
Vista nine		not installed	on disk
Vista eight		not installed	on disk

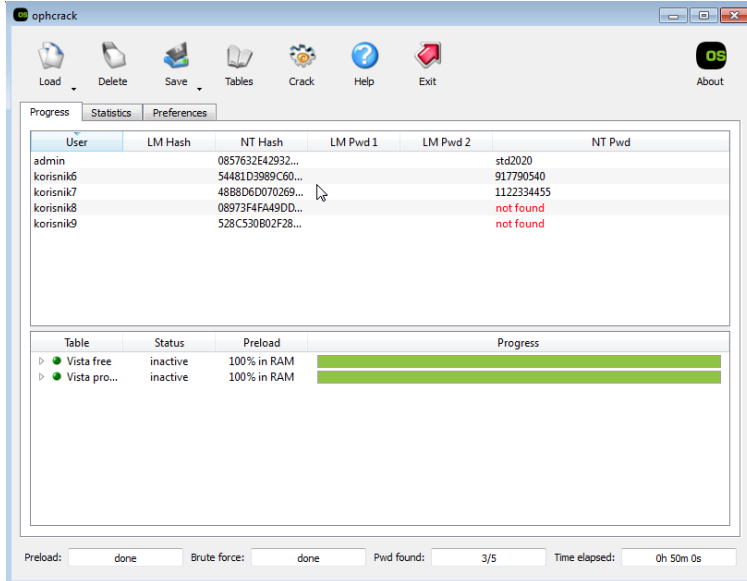
27. Kliknuti na Crack i pustiti da se razbijaju lozinke. Očekivano vreme ovog pokušaja razbijanja lozinki je oko dvanaest minuta. Primetiti da su jednostavnije lozinke pronađene, a neke komplikovanije i duže nisu.



28. Dodati drugu tabelu sa desktopa (Vista proba free) na isti naćin kao i prethodnu.


29. Ukloniti korisnike za koje je lozinka pronađena.

30. **Ukloniti korisnika 8 i 9 iz liste**, jer ni ova rainbow tabela neće pomoći u razbijanju njihovih šifri, a vreme potrebno samo za prolazak kroz ove dve rainbow tabele je oko pedeset minuta, ali možete da verujete slici koja se nalazi ispod ☺. Pokrenuti razbijanje lozinke klikom na dugme crack. Oćekivano vreme razbijanja za ove tri lozinke je oko trideset sekundi.




31. Otvoriti web stranicu [Objectif Sécurité](http://Objectif_Sécurité) (svejedno da li je sa virtuelne mašine ili lokalnog kompjutera) i popuniti lozinku u donjem polju tako da od nje dobijete heš.

DEMO

Last 5 hashes tested 


Hash	Result	Cracking time
e5c71a17d00b1be3cd7c70433d944319	-	228 s
6aa13b04e403ba9541d1c2e59e24a653	-	234 s
b70148f6cc82e8e5e01f958b620520c0	u1	6 s
17e328fdd32682ecfa24a6ccfe61dcad	u0	6 s
e88f9e24763fbcc63ad6ea2c0bfd1fef	-	221 s

 Your hash is in the cracking queue at position 1

The NTHash of the password submitted is 528c530b02f2833331c0f7c5d97bebc5

32. Pritisnuti na Go i ispod će se izgenerisati heš. Taj heš prekopirati u gornje polje i pritisnuti go.
33. Nakon tri do četiti minuta rezultat će biti ovakav, lozinka nije pronađena

DEMO

Last 5 hashes tested 

Hash	Result	Cracking time
e5c71a17d00b1be3cd7c70433d944319	-	228 s
6aa13b04e403ba9541d1c2e59e24a653	-	234 s
b70148f6cc82e8e5e01f958b620520c0	u1	6 s
17e328fdd32682ecfa24a6ccfe61dcad	u0	6 s
e88f9e24763fbcc63ad6ea2c0bfd1fef	-	221 s

Cracking result: Password not found

The NTHash of the password submitted is 528c530b02f2833331c0f7c5d97bebc5

34. Ponoviti korake 30-32 sa lozinkom 1122334455a. Ova lozinka će biti pronađena.

7.4 Korišćenje podrazumevanih lozinki:

Većina računarske opreme: ruteri, modemi, računari, itd. uglavnom dolazi prekonfigurisana sa podrazumevanom lozinkom. Ponekad je slučaj da proizvođač eksplicitno traži promenu lozinke prilikom prvog logovanja na sistem, ali najčešće to nije situacija.

Uzmite neki svoj uređaj (npr. kućni ruter), pogledajte ko je proizvođač i koji je model uređaja (npr. Asus 6310EV). Pronađite podrazumevane lozinke za taj uređaj:

1. Idite na sajt <http://www.passwordsdatabase.com/>
2. Odaberite vendora vašeg modema – Asus
3. Pogledajte koja je podrazumevana lozinka i korisničko ime
4. Probajte da li vašem kućnom ruteru može da se pristupi preko te lozinke (ako može da se pristupi i ako je to podešavanje koje je postavio Vaš provajder, nemojte da menjate bez njihovog znanja)