

KEAMANAN JARINGAN DAN KOMPUTER
DUMPING AND CRACKING SAM HASHES TO EXTRACT
PLAINTEXT PASSWORDS



Disusun oleh :

Nama : Viona Aulia Meidy

NIM : 09011282126075

Kelas : SK7A Indralaya

UNIVERSITAS SRIWIJAYA
FAKULTAS ILMU KOMPUTER
SISTEM KOMPUTER

2024

1. Buka command prompt lalu klik run as administrator, masukkan perintah “wmic useraccount get name, sid”, setelah setelah lakukan penginstallan pwdump dan pindahkan pada desktop. Selanjutnya, salin Lokasi file pwdump lalu buat perintah di command prompt “cd C:\Users\USER\Desktop\pwdump7”, jika selesai lanjutkan dengan menuliskan perintah PwDump7.exe kemudian lakukan enter. Terakhir, lakukan perintah “PwDump7.exe > C:\hashes.txt” dan file hashes.txt akan tersimpan pada desktop. Berikut adalah perintah yang dijalankan pada command prompt :

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.22631.4317]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>wmic useraccount get name, sid
Name                SID
Administrator       S-1-5-21-3604377980-3503621335-2773563393-500
DefaultAccount       S-1-5-21-3604377980-3503621335-2773563393-503
Guest                S-1-5-21-3604377980-3503621335-2773563393-501
USER                 S-1-5-21-3604377980-3503621335-2773563393-1001
WDAGUtilityAccount   S-1-5-21-3604377980-3503621335-2773563393-504

C:\Windows\System32>cd C:\Users\USER\Desktop\pwdump7

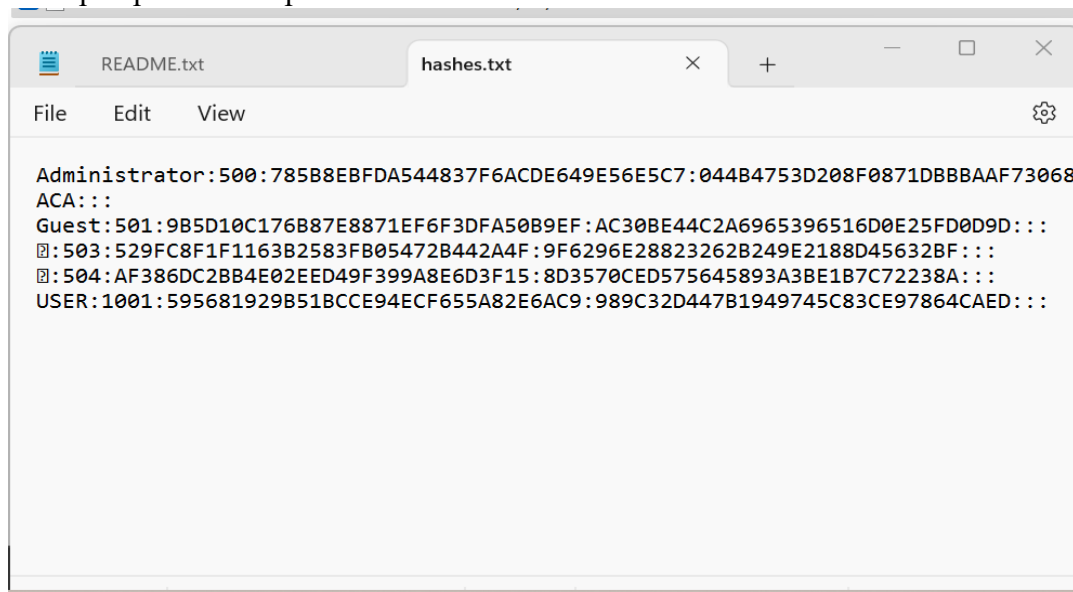
C:\Users\USER\Desktop\pwdump7>PwDump7.exe
PwDump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

Administrator:500:785B8EBFDA544837F6ACDE649E56E5C7:044B4753D208F0871DBBBAAF73068ACA:::
Guest:501:9B5D10C176B87E8871EF6F3DFA50B9EF:AC30BE44C2A6965396516D0E25FD0D9D:::
j:503:529FC8F1F1163B2583FB05472B442A4F:9F6296E28823262B249E2188D45632BF:::
j:504:AF386DC2BB4E02EED49F399A8E6D3F15:8D3570CED575645893A3BE1B7C72238A:::
USER:1001:595681929B51BCCE94ECF655A82E6AC9:989C32D447B1949745C83CE97864CAED:::

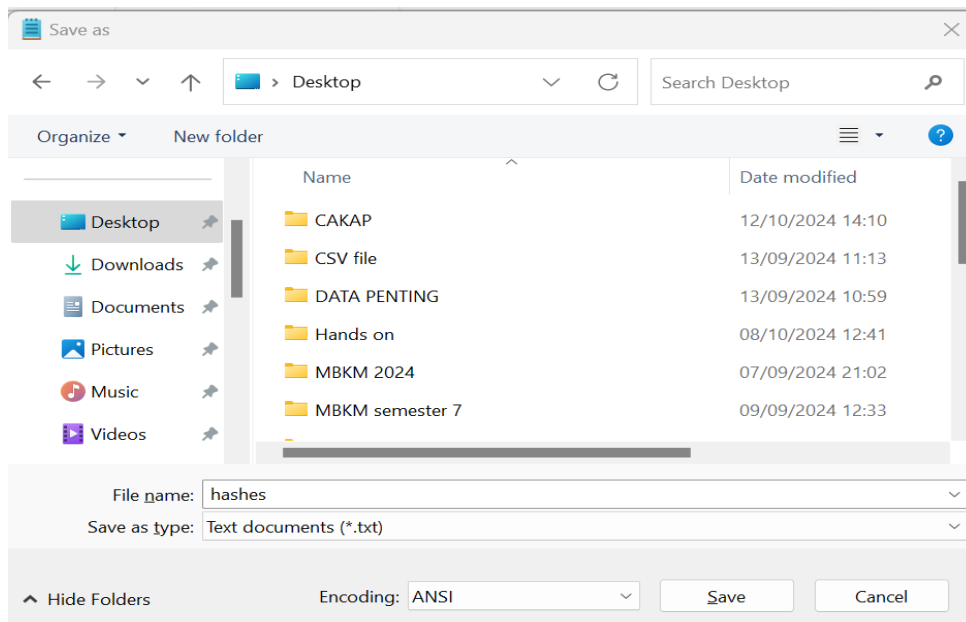
C:\Users\USER\Desktop\pwdump7>PwDump7.exe > C:\hashes.txt
PwDump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

C:\Users\USER\Desktop\pwdump7>
```

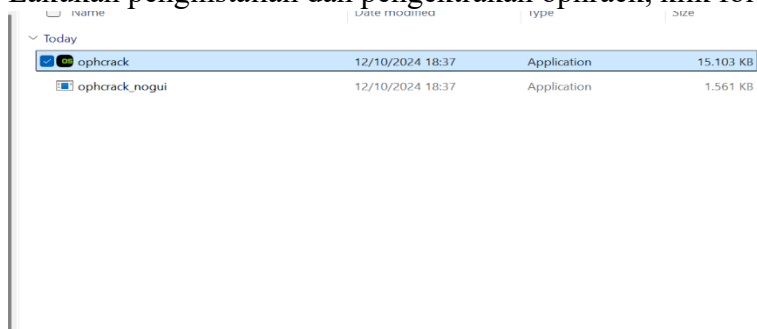
2. Buka file hashes.txt dengan menggunakan notepad, lakukan penyimpanan dan disimpan pada desktop.



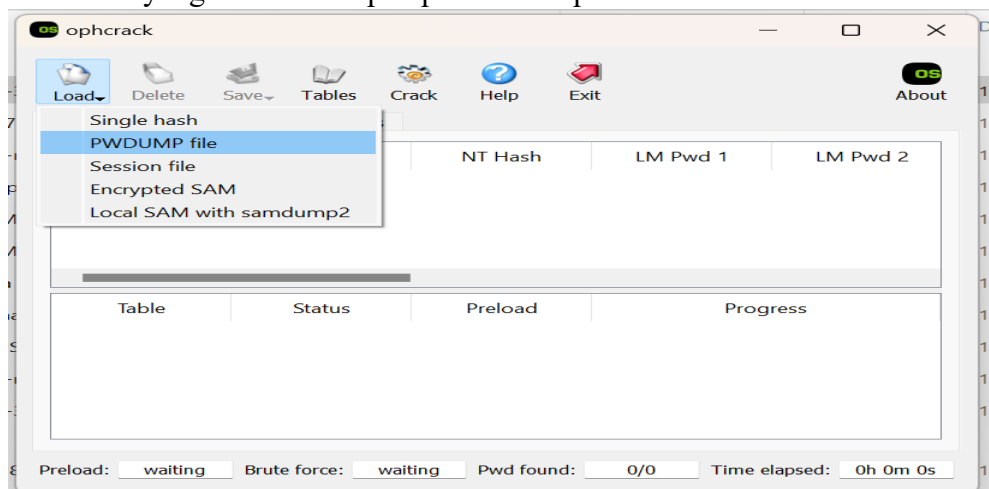
```
Administrator:500:785B8EBFDA544837F6ACDE649E56E5C7:044B4753D208F0871DBBBAAF73068ACA:::
Guest:501:9B5D10C176B87E8871EF6F3DFA50B9EF:AC30BE44C2A6965396516D0E25FD0D9D:::
j:503:529FC8F1F1163B2583FB05472B442A4F:9F6296E28823262B249E2188D45632BF:::
j:504:AF386DC2BB4E02EED49F399A8E6D3F15:8D3570CED575645893A3BE1B7C72238A:::
USER:1001:595681929B51BCCE94ECF655A82E6AC9:989C32D447B1949745C83CE97864CAED:::
```

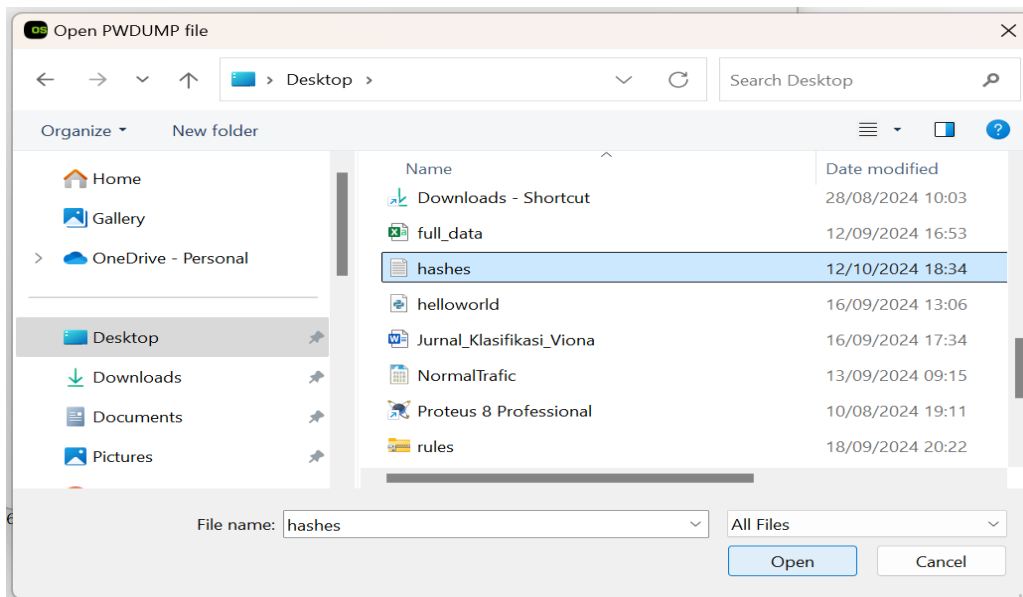


- Lakukan penginstallan dan pengekrakan ophcrack, klik folder dan klik opcrack.exe

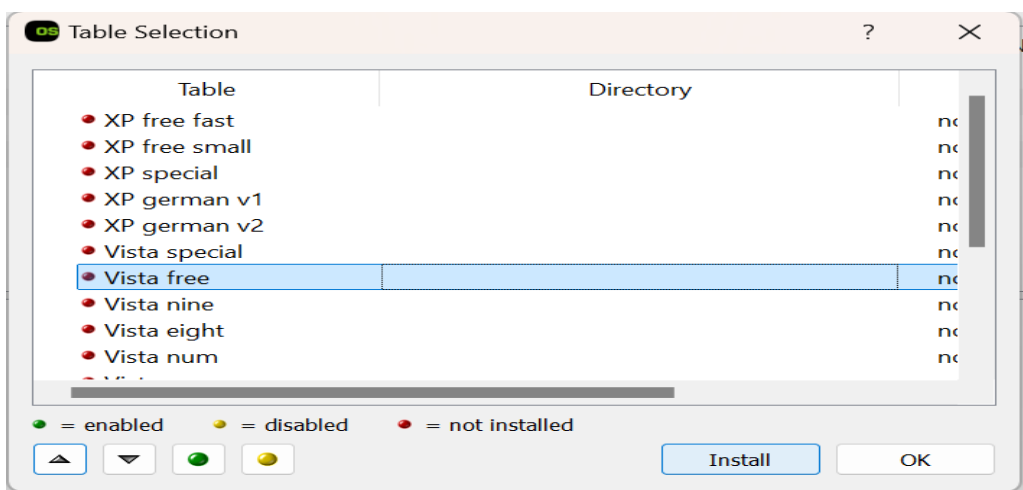
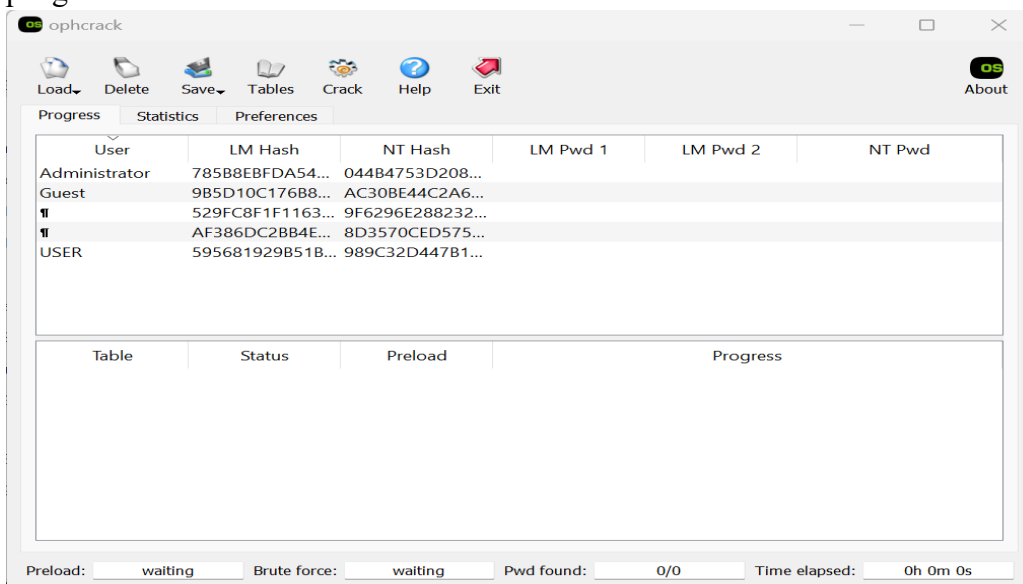


- Tampilan akan masuk kedalam ophcrack, klik load lalu pilih PWDUMP file, cari file hashes.txt yang sudah disimpan pada desktop.

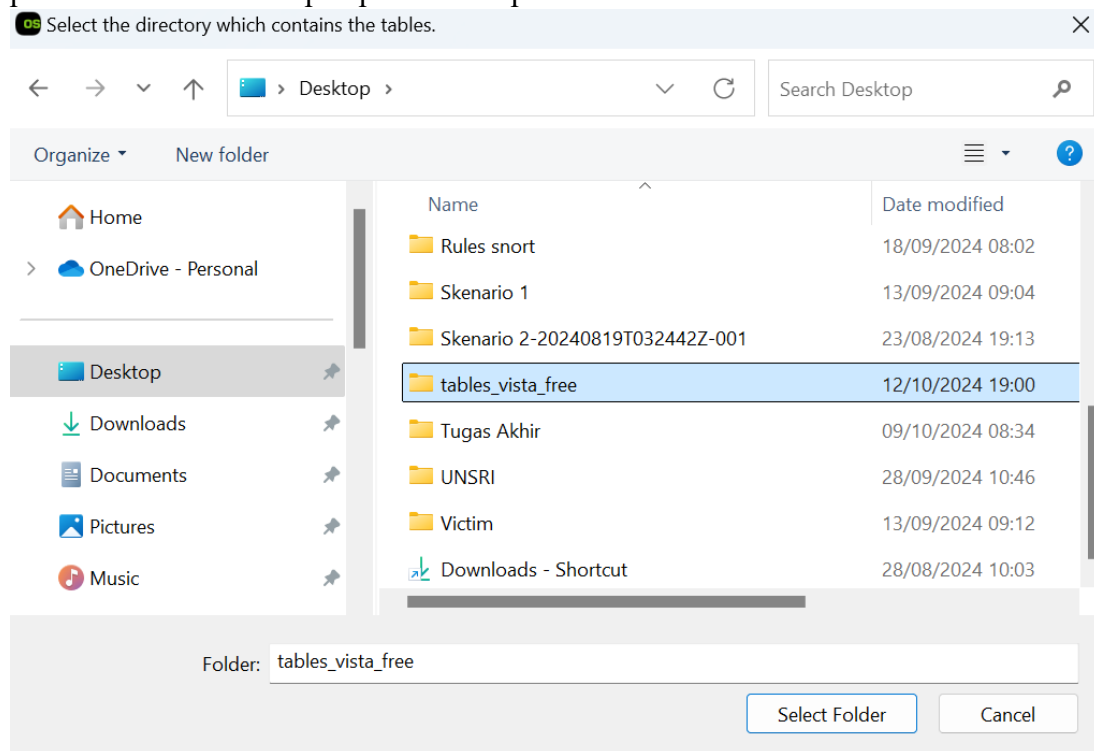




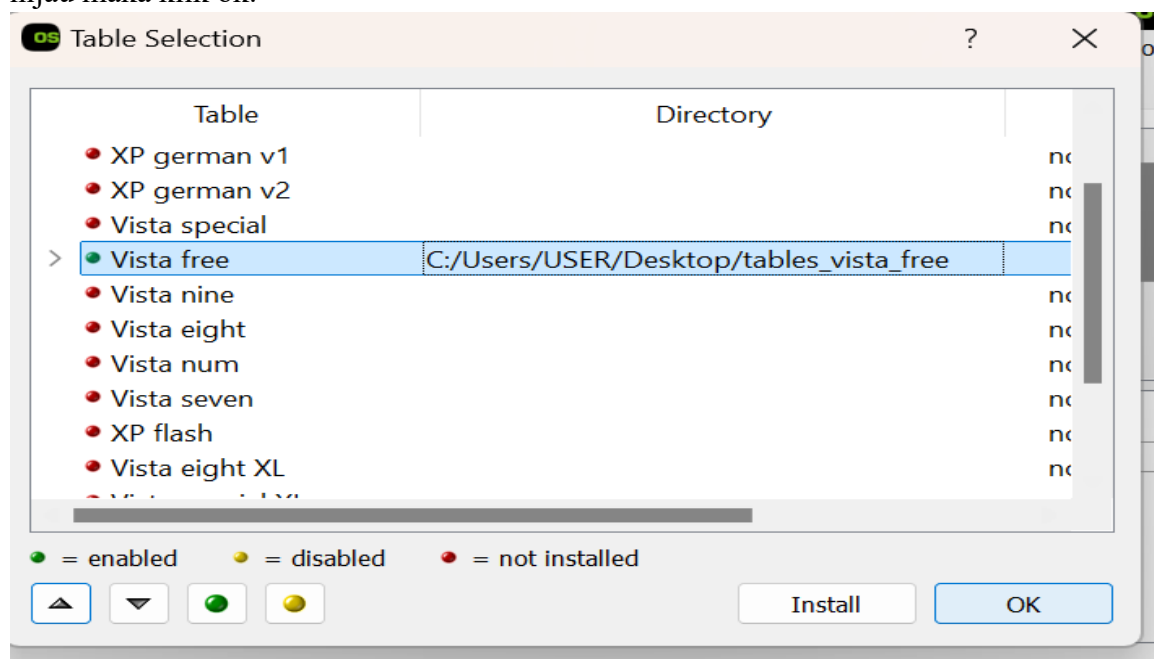
- File hashes.txt akan tampil pada ophrack, lakukan penginstalan vista free yang berada dalam website ophrack, setelah selesai klik tables dan pilih vista free dan lakukan penginstalan.



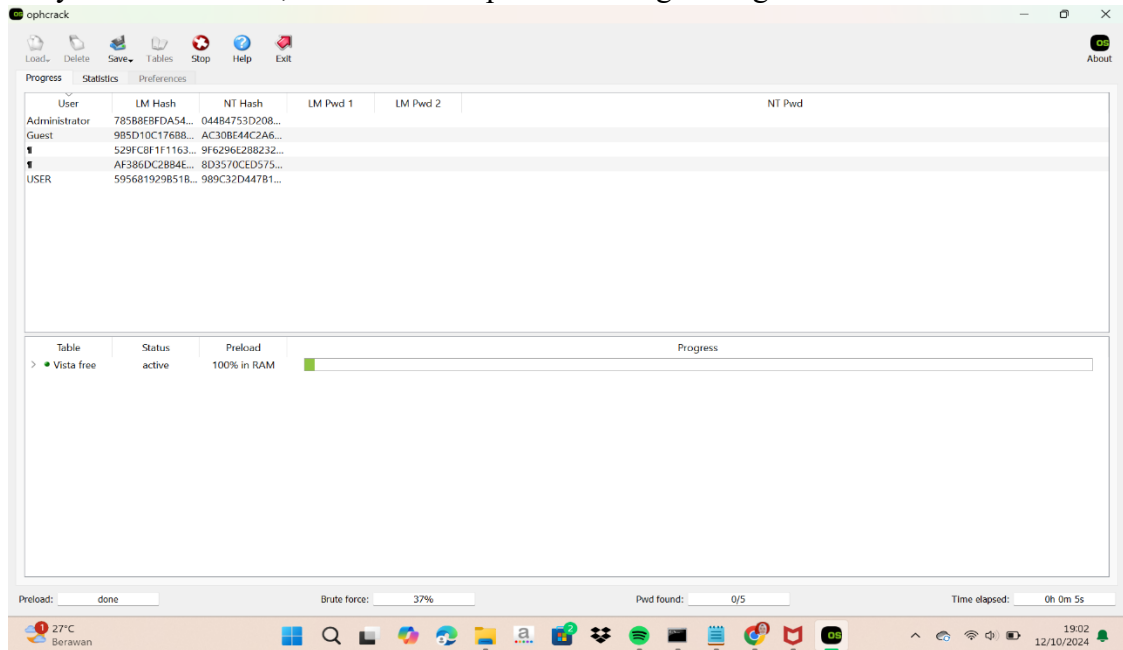
6. Penginstallan disimpan sesuai dengan tempat tables_visit_free disimpan, dalam percobaan folder disimpan pada desktop.



7. Penginstallan akan berhasil jika vista free telah berwarna hijau, jika vista free berwarna hijau maka klik ok.



8. Penyelesaian terakhir, klik crack dan proses loading sedang dilakukan.



9. Proses telah selesai dilakukan dan tampilan yang ditunjukkan adalah sebagai berikut :

