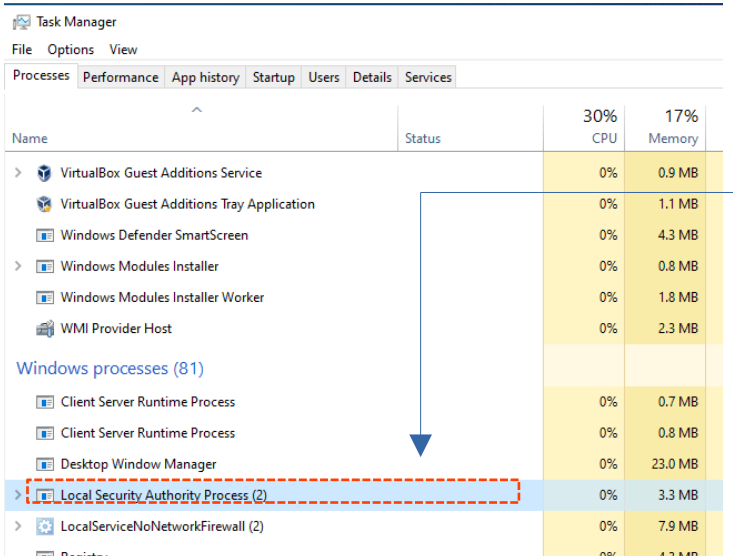
Password Stealing from LSASS

LSASS (Local Security Authority Server Service)

- **Role**: It's a critical Windows process responsible for handling authentication, enforcing security policies, and managing user logins.
- Path: C:\Windows\System32\lsass.exe
- Sensitive data in memory: NTLM hashes

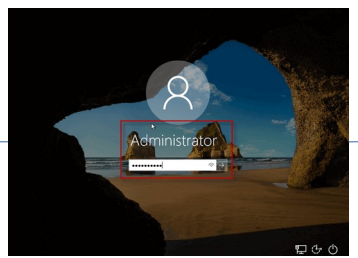
LSASS (Local Security Authority Server Service)



lsass.exe

When a user logs into a system, LSASS verifies the credentials and keeps sensitive information like passwords and authentication tokens in memory.

Win OS



Login

User