

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)

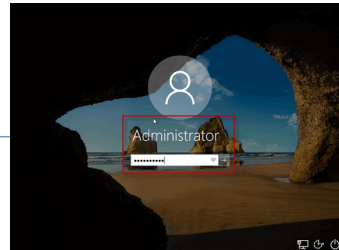
Name	Status	30% CPU	17% Memory
> VirtualBox Guest Additions Service		0%	0.9 MB
VirtualBox Guest Additions Tray Application		0%	1.1 MB
Windows Defender SmartScreen		0%	4.3 MB
> Windows Modules Installer		0%	0.8 MB
Windows Modules Installer Worker		0%	1.8 MB
WMI Provider Host		0%	2.3 MB
Windows processes (81)			
Client Server Runtime Process		0%	0.7 MB
Client Server Runtime Process		0%	0.8 MB
Desktop Window Manager		0%	23.0 MB
Local Security Authority Process (2)		0%	3.3 MB
> LocalServiceNoNetworkFirewall (2)		0%	7.9 MB

Isass.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