

How can we steal the password from lsass process ?

# Password stealing from lsass.exe process :

```
BOOL MiniDumpWriteDump(  
HANDLE hProcess,  
DWORD ProcessId,  
HANDLE hFile,  
MINIDUMP_TYPE DumpType,  
PMINIDUMP_EXCEPTION_INFORMATION ExceptionParam,  
PMINIDUMP_USER_STREAM_INFORMATION UserStreamParam,  
PMINIDUMP_CALLBACK_INFORMATION CallbackParam  
);
```

The **MiniDumpWriteDump** function is a Windows API provided by DbgHelp.dll. It allows a process to create a minidump file, which is a snapshot of another process's memory and state at a specific point in time.

The screenshot shows the Windows Task Manager interface with the 'Processes' tab selected. The list of processes includes various system services and applications. The 'Local Security Authority Process (2)' is highlighted with a red dashed box, indicating it is the target of the password-stealing operation. An arrow points from the code block to this process.

Name	Status	30% CPU	17% Memory	3% Disk	0% Network	Power usage
> VirtualBox Guest Additions Service		0%	0.9 MB	0 MB/s	0 Mbps	Very low
VirtualBox Guest Additions Tray Application		0%	1.1 MB	0 MB/s	0 Mbps	Very low
Windows Defender SmartScreen		0%	4.3 MB	0 MB/s	0 Mbps	Very low
> Windows Modules Installer		0%	0.8 MB	0 MB/s	0 Mbps	Very low
Windows Modules Installer Worker		0%	1.8 MB	0 MB/s	0 Mbps	Very low
WMI Provider Host		0%	2.3 MB	0 MB/s	0 Mbps	Very low
Windows processes (81)						
Client Server Runtime Process		0%	0.7 MB	0 MB/s	0 Mbps	Very low
Client Server Runtime Process		0%	0.8 MB	0 MB/s	0 Mbps	Very low
Desktop Window Manager		0%	23.0 MB	0 MB/s	0 Mbps	Very low
> Local Security Authority Process (2)		0%	3.3 MB	0 MB/s	0 Mbps	Very low
> LocalServiceNoNetworkFirewall (2)		0%	7.9 MB	0 MB/s	0 Mbps	Very low
Registry		0%	4.3 MB	0 MB/s	0 Mbps	Very low
> Service Host: Application Information		0%	0.8 MB	0 MB/s	0 Mbps	Very low
> Service Host: Background Intelligent Transfer Service		0%	2.7 MB	0 MB/s	0 Mbps	Very low
> Service Host: Capability Access Manager Service		0%	1.0 MB	0 MB/s	0 Mbps	Very low
> Service Host: Clipboard User Service_46614		0%	1.7 MB	0 MB/s	0 Mbps	Very low
> Service Host: COM+ Event System		0%	1.5 MB	0 MB/s	0 Mbps	Very low
> Service Host: Connected Devices Platform Service		0%	2.7 MB	0 MB/s	0 Mbps	Very low

# Password stealing from lsass.exe process :

```
BOOL MiniDumpWriteDump(  
HANDLE hProcess,  
DWORD ProcessId,  
HANDLE hFile,  
MINIDUMP_TYPE DumpType,  
PMINIDUMP_EXCEPTION_INFORMATION ExceptionParam,  
PMINIDUMP_USER_STREAM_INFORMATION UserStreamParam,  
PMINIDUMP_CALLBACK_INFORMATION CallbackParam  
);
```

Get the process id of lsass.exe

Name	Status	30% CPU	17% Memory	3% Disk	0% Network	Power usage
> VirtualBox Guest Additions Service		0%	0.9 MB	0 MB/s	0 Mbps	Very low
VirtualBox Guest Additions Tray Application		0%	1.1 MB	0 MB/s	0 Mbps	Very low
Windows Defender SmartScreen		0%	4.3 MB	0 MB/s	0 Mbps	Very low
> Windows Modules Installer		0%	0.8 MB	0 MB/s	0 Mbps	Very low
Windows Modules Installer Worker		0%	1.8 MB	0 MB/s	0 Mbps	Very low
WMI Provider Host		0%	2.3 MB	0 MB/s	0 Mbps	Very low
Windows processes (81)						
Client Server Runtime Process		0%	0.7 MB	0 MB/s	0 Mbps	Very low
Client Server Runtime Process		0%	0.8 MB	0 MB/s	0 Mbps	Very low
Desktop Window Manager		0%	23.0 MB	0 MB/s	0 Mbps	Very low
> Local Security Authority Process (2)		0%	3.3 MB	0 MB/s	0 Mbps	Very low
> LocalServiceNoNetworkFirewall (2)		0%	7.9 MB	0 MB/s	0 Mbps	Very low
Registry		0%	4.3 MB	0 MB/s	0 Mbps	Very low
> Service Host: Application Information		0%	0.8 MB	0 MB/s	0 Mbps	Very low
> Service Host: Background Intelligent Transfer Service		0%	2.7 MB	0 MB/s	0 Mbps	Very low
> Service Host: Capability Access Manager Service		0%	1.0 MB	0 MB/s	0 Mbps	Very low
> Service Host: Clipboard User Service_46614		0%	1.7 MB	0 MB/s	0 Mbps	Very low
> Service Host: COM+ Event System		0%	1.5 MB	0 MB/s	0 Mbps	Very low
> Service Host: Connected Devices Platform Service		0%	2.7 MB	0 MB/s	0 Mbps	Very low