Red Team/Blue Team Practice on Wdigest

hackingarticles.in/red-team-blue-team-practice-on-wdigest

Raj February 14, 2019

In this article, we will show you the methods of protecting your system against MIMIKATZ that fetches password in clear text from wdigest. As you know the Pen-tester and the red team uses mimikatz for testing password capacity. For the complete information on how mimikatz works visit this link:

https://www.hackingarticles.in/understanding-guide-mimikatz/

Table of Contents

Introduction of WDigest

WDigest.dll was introduced in the Windows XP operating system. in Windows XP, Microsoft added support for a protocol known as WDigest. The WDigest protocol is used for clients to send clear text credentials to Hypertext Transfer Protocol (HTTP) and Simple Authentication Security Layer (SASL) applications based on RFC 2617 and 2831. When the WDigest authentication protocol is enabled, clear text password is stored, where it can be at risk of theft.

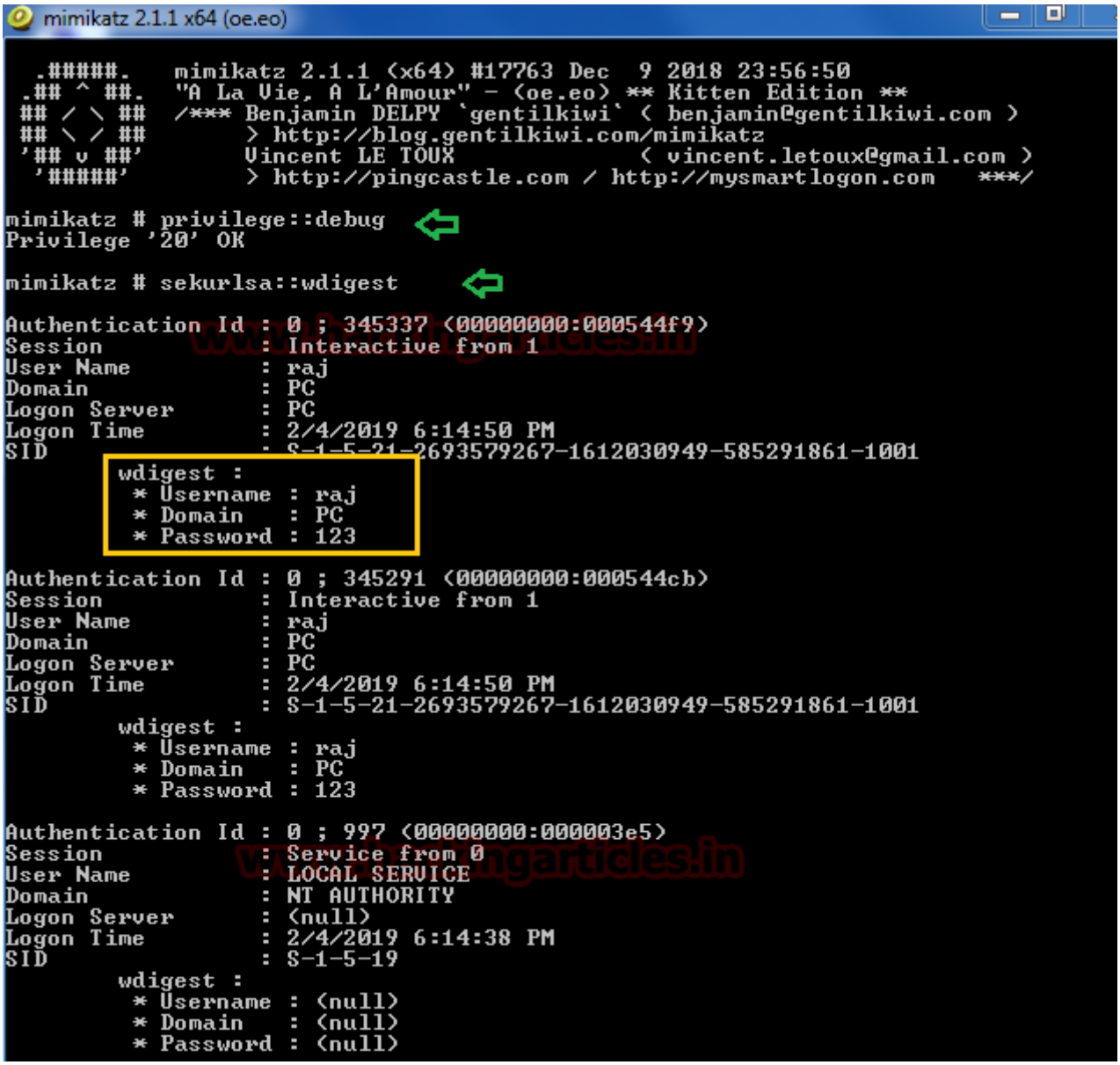
System Impacted

The problem with WDigest is that it stores passwords in memory in clear-text and it can be extracted by using MIMIKATZ. The following OS's are impacted: Windows 7, Windows 8, Windows 8.1, Windows Server 2008, Windows Server 2008R2, and Windows Server 2012.

Demonstration on windows 7

An attacker with administrator privileges can steal credentials from damaged system memory. Memory credentials are stored in plain text and in various hash formats. First, we will demonstrate how we can see the password of Windows 7 using MIMIKATZ tool as shown in the image below as it has shown the password in the clear text. And for this, we will following commands in MIMIKATZ tool

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

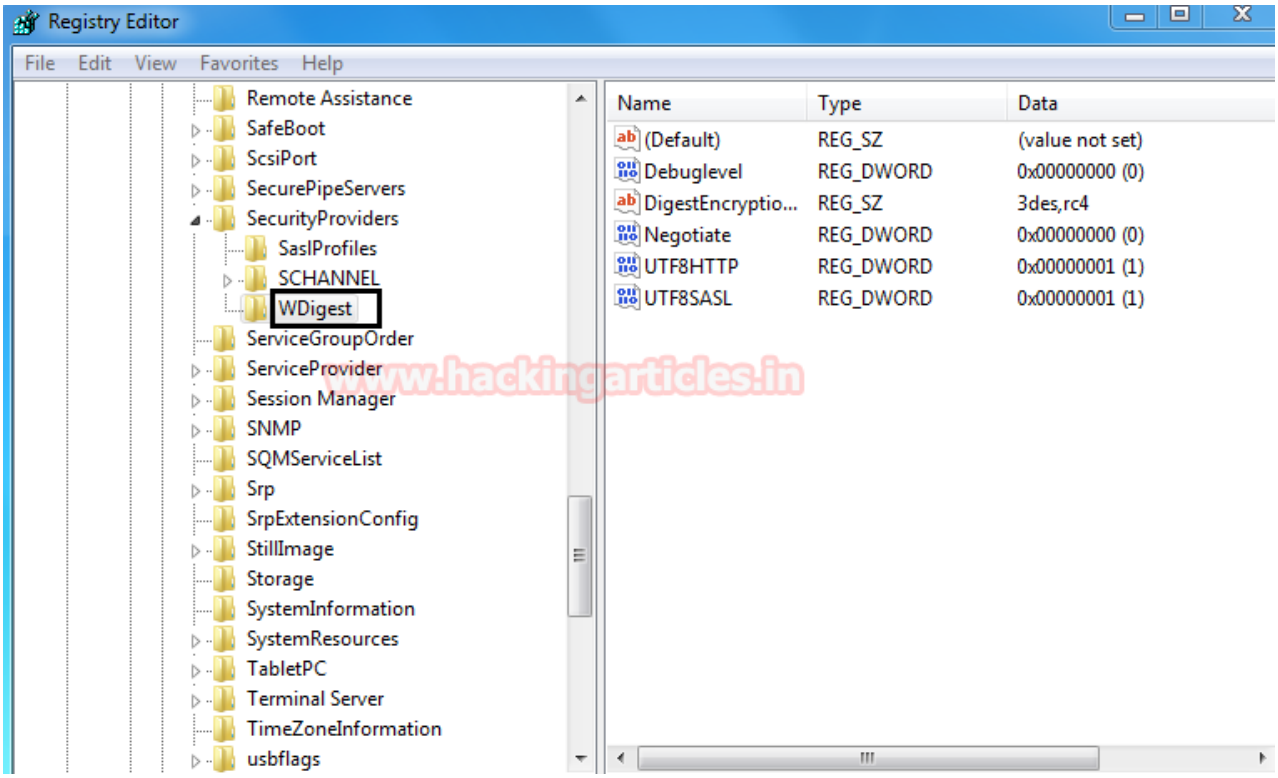


Now as you can observe that is has shown you the password in clear text. We can also do this by taking the meterpreter of the target system and then using MIMIKATZ in Kali. Here you will see that it has also shown us the password of the compromised system.

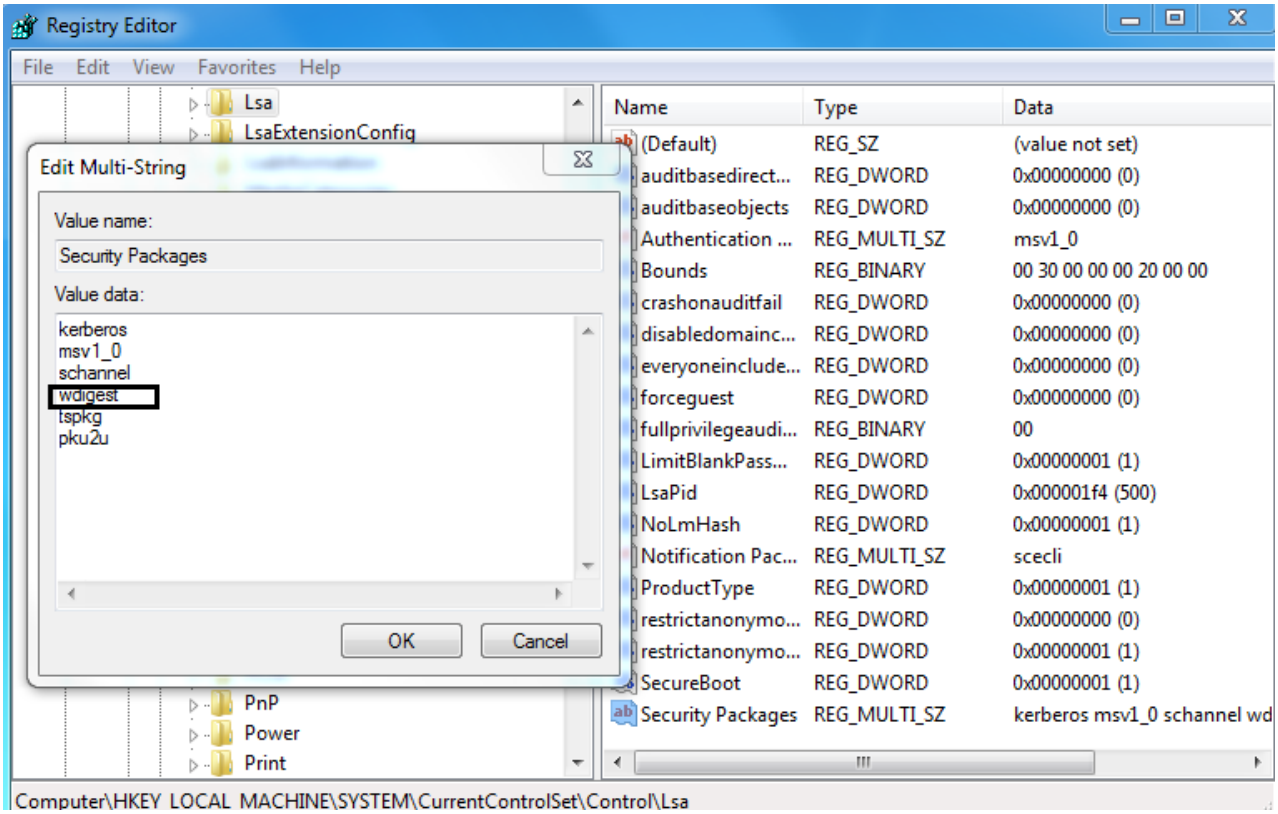
Disable WDigest (Defending against Mimikatz)

Now as we know that it is a security threat; so now we will get to know how we can remove this from our system and for this a registry change is required to make to hide our password. For this, we will first open the regedit and then go to WDigest option using the following path

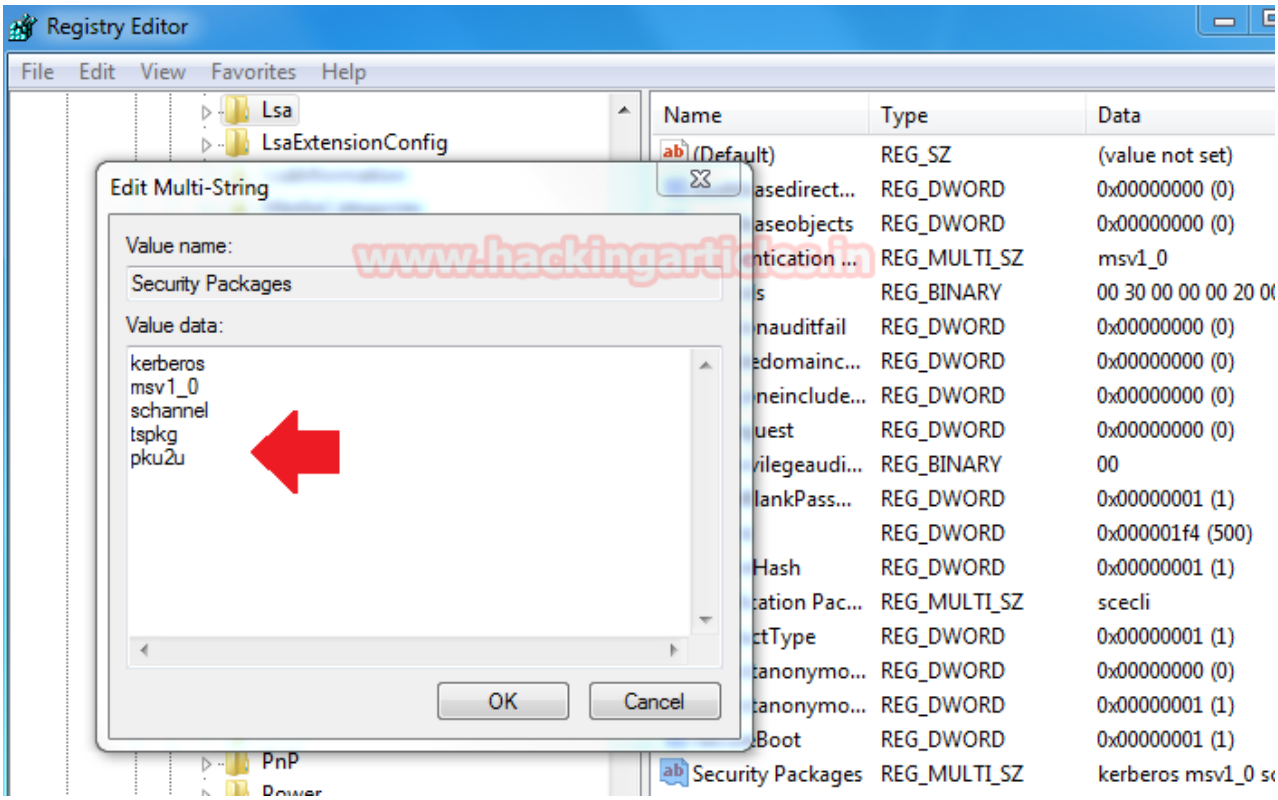
```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\WDigest
```



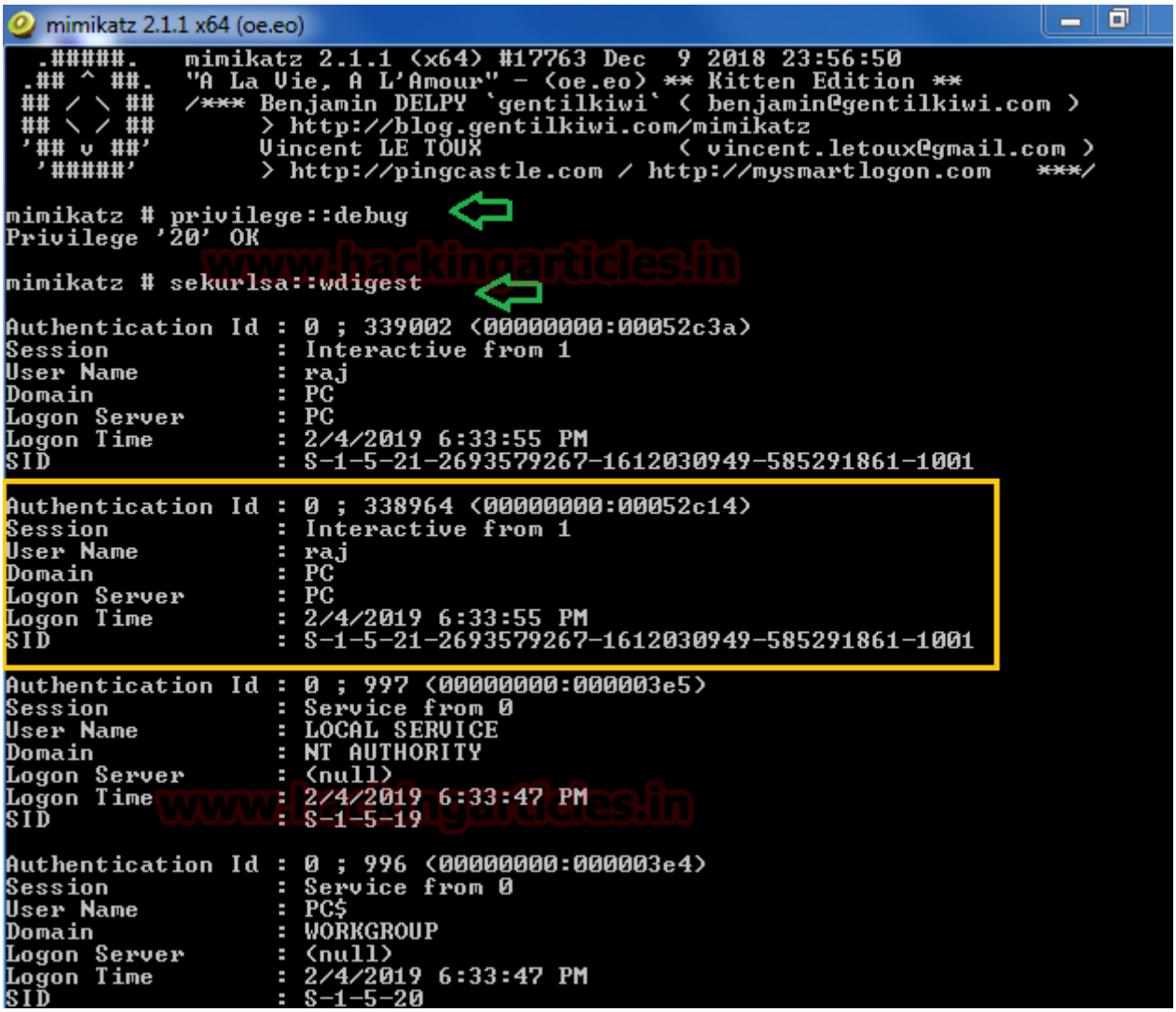
Here you need to open the security packages and you will see WDigest with the other options as shown in the image below



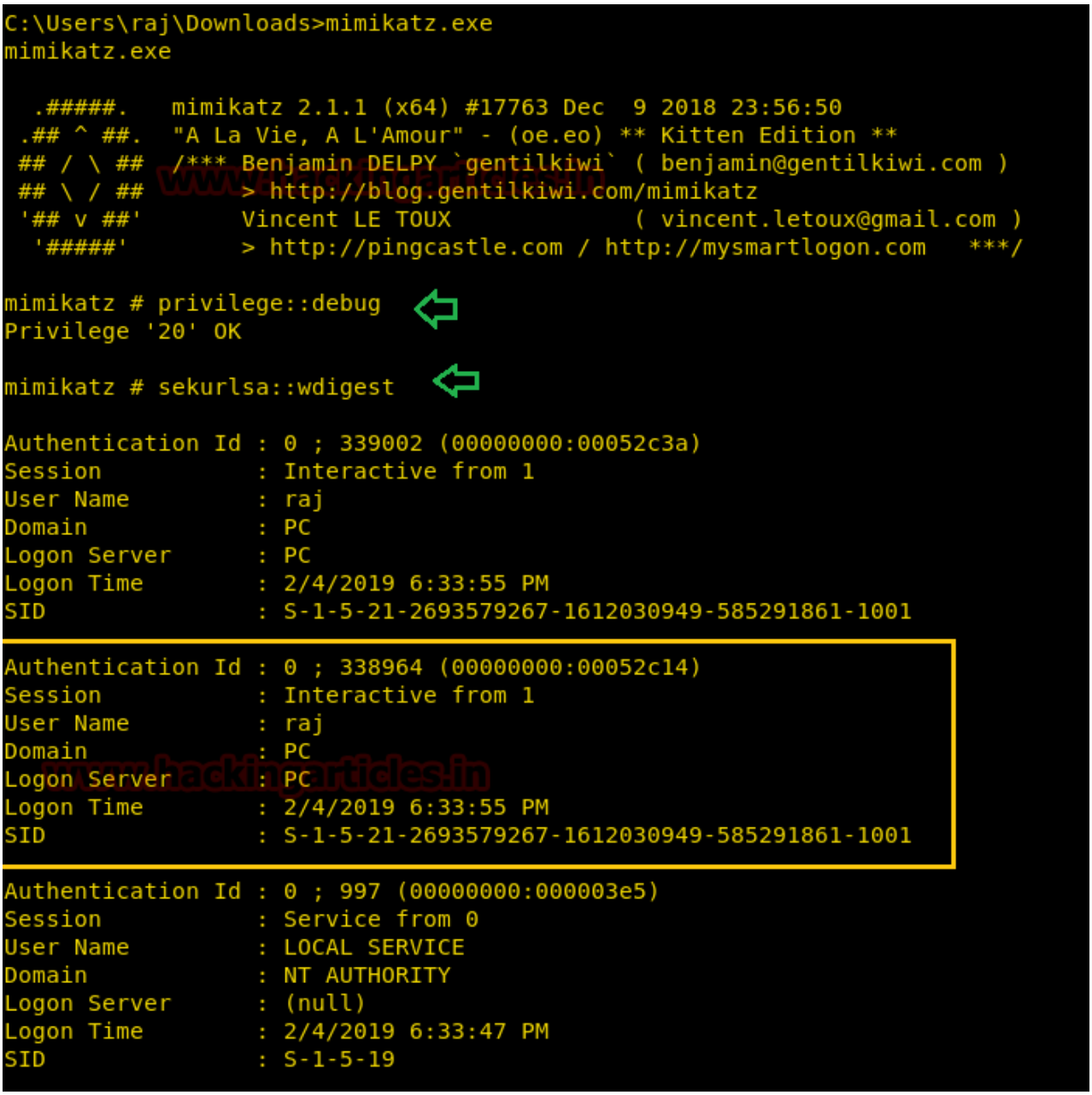
Great! You have found that. Now simply you need to remove **Wdigest** from here so that nobody can see the password using MIMIKATZ tool.



Now after making these changes, we need to update the group policy and reboot the system. After doing so we will again use **MIMIKATZ** tool to see the change now. So we will use the same commands which we have used earlier to get the password and this time it will show us the password **NULL** as shown in the image.

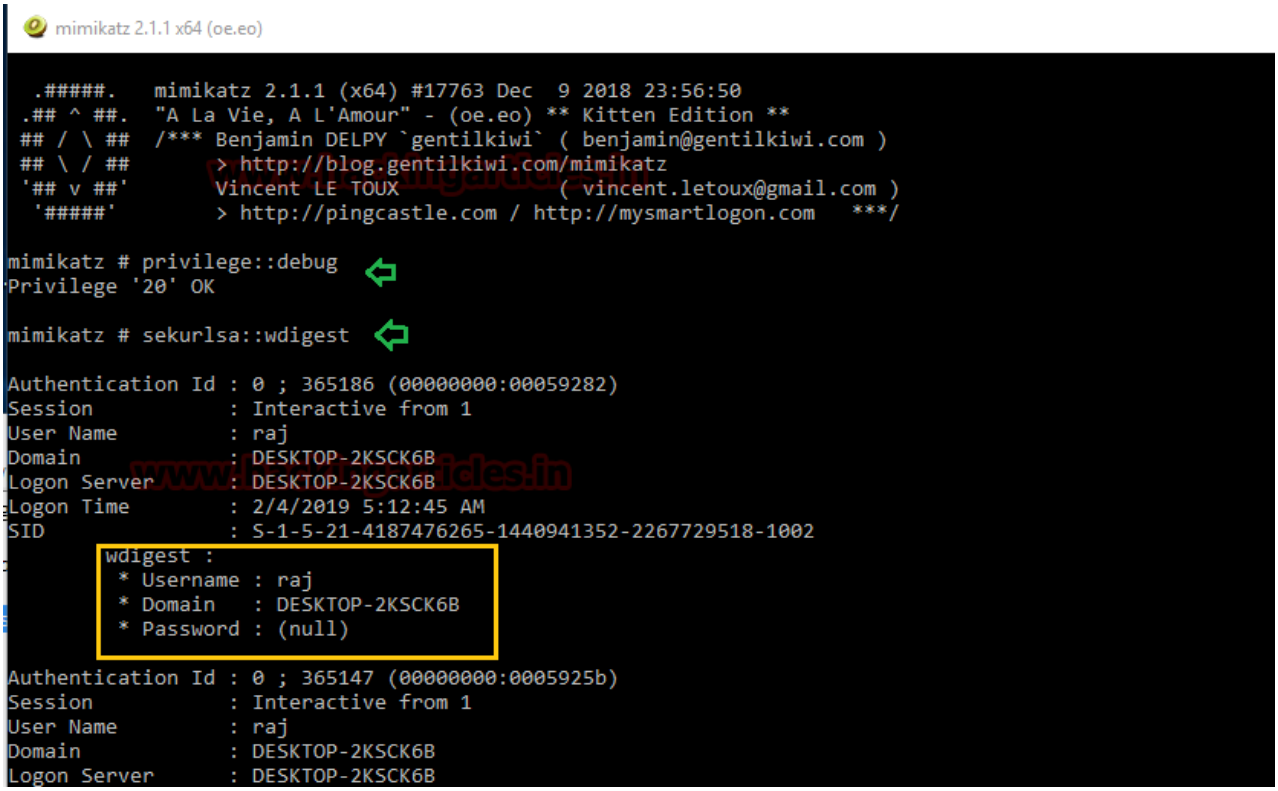


Great! We have successfully hidden the password. Now, if somebody has taken the meterpreter of the Windows 7 and if the attacker tries this in kali using **MIMIKATZ** tool there. Even then the attacker is not able to get the password of the compromised system as shown in the image below



Demonstration on Windows 10

In the same way, we will try this method in **Windows 10** and as we know that in **Windows 10** it is disabled by default. We can verify this by using the **MIMIKATZ** tool there.

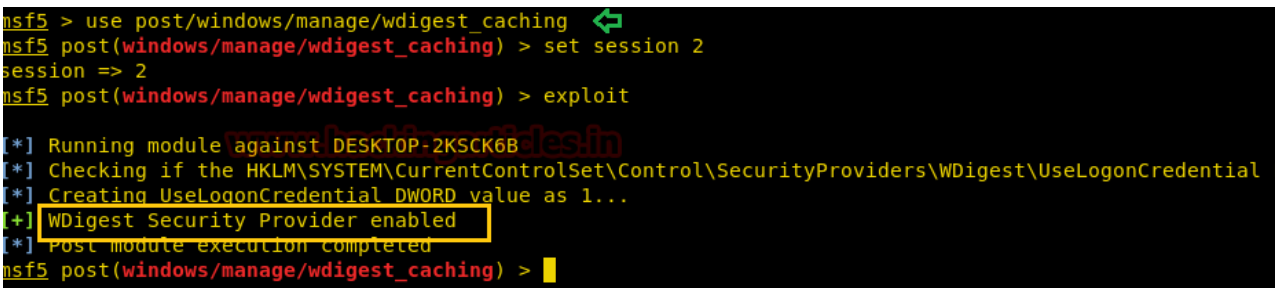


Enable WDigest in Windows 10

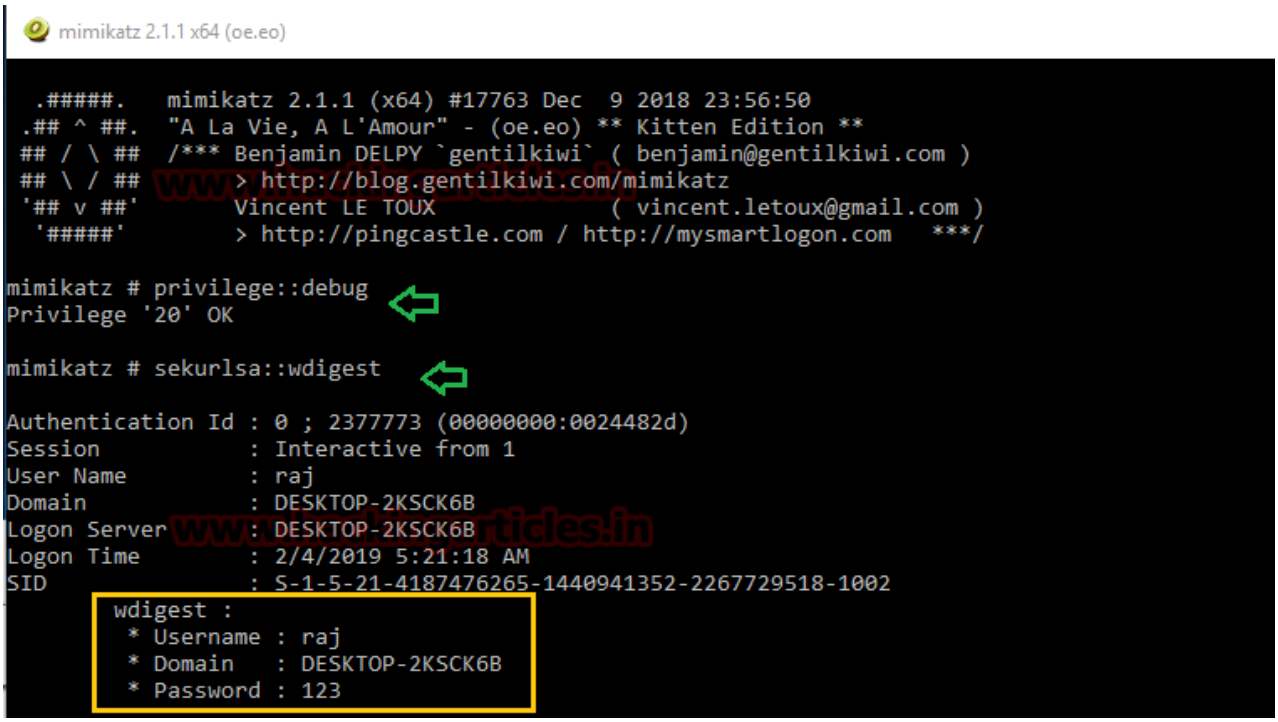
Yes; as we have verified that the **Wdigest** option is disabled by default. Now we will learn how we can enable **Wdigest** in Windows 10. For this first, we need to take meterpreter of the target system and then we need to take the admin access of the system and then we need to use the exploit to enable **Wdigest** in the target system with the help of the following module.

On Windows 8/2012 or higher, the Digest Security Provider (WDIGEST) is disabled by default. This module enables/disables credential caching by adding/changing the value of the UseLogonCredential DWORD under the WDIGEST provider's Registry key. Any subsequent logins will allow mimikatz to recover the plain text passwords from the system's memory.

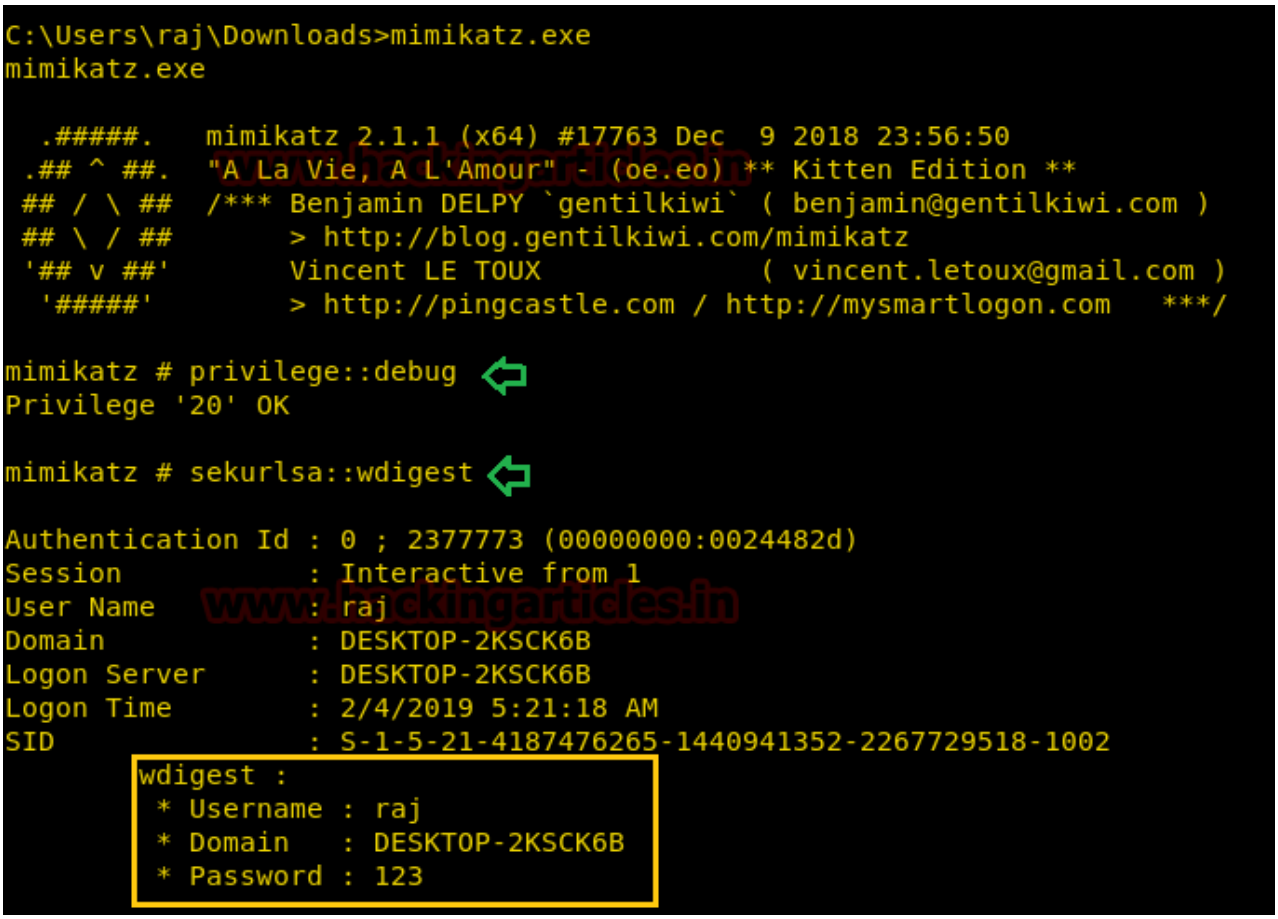
```
use post/windows/manage/wdigest_caching
msf post(windows/manage/wdigest_caching) > set session 2
msf post(windows/manage/wdigest_caching) > exploit
```



After making the changes we will check if the **Wdigest** option is enabled. For this, we will again use **MIMIKATZ** tool here and we will observe that we have found the password of the victim's P.C



We can do this too by taking the meterpreter of the system using **MIMIKATZ** tool there.

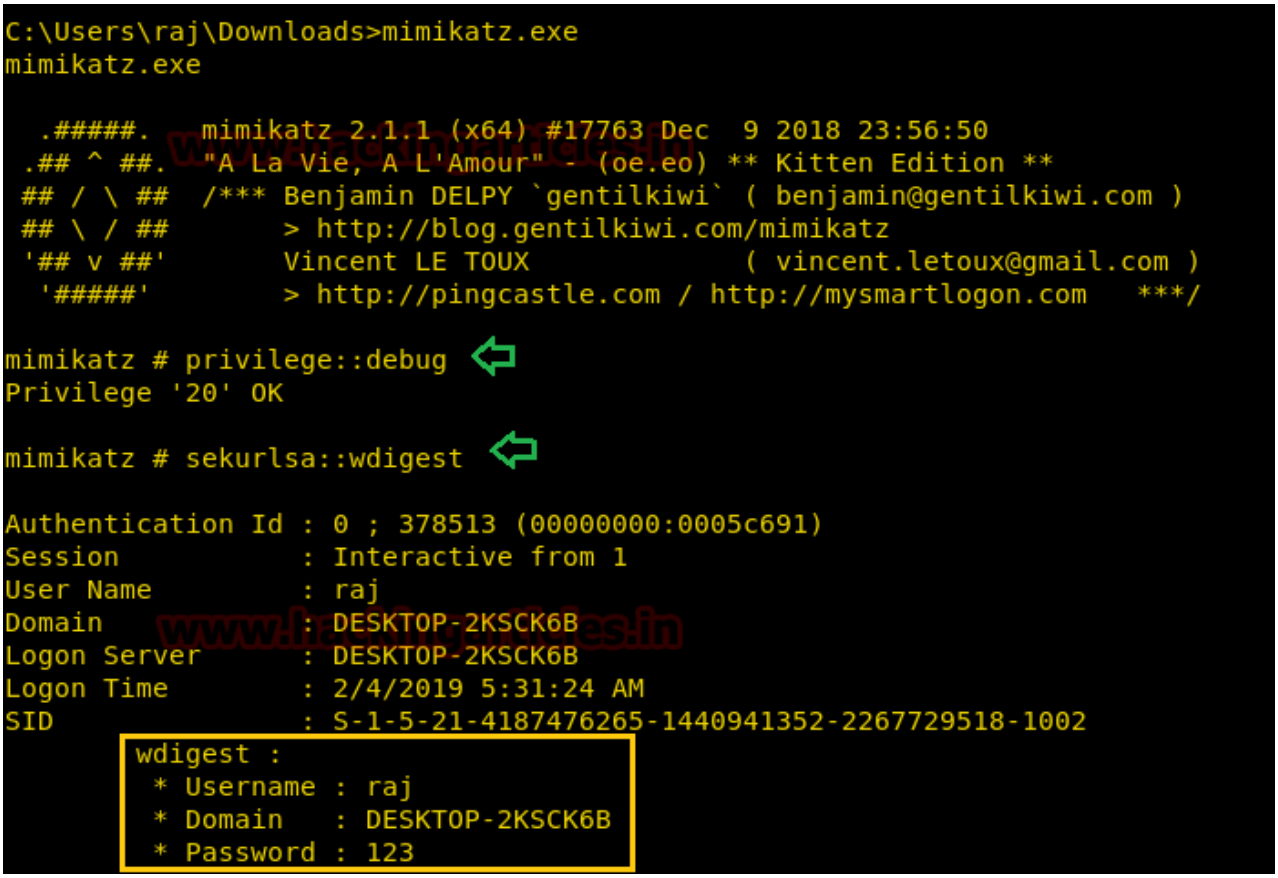


Enable Wdigest via a registry key

There is one more way to see the password. The second method to enable WDigest is by taking the shell of the compromised system. Now run the following command to enable the wdigest.

```
reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v
UseLogonCredential /t REG_DWORD /d 1
```

After you get the shell; you need to run **Mimikatz** tool here and we will use the same commands to see the password. And you will observe that we have got the password.



Excellent we have done this with this method also. And we know that how to see the password in **Windows 10** and how to enable and disable that.

Author: Geet Madan is a Certified Ethical Hacker, Researcher and Technical Writer at Hacking Articles on Information Security**.** Contact **here**