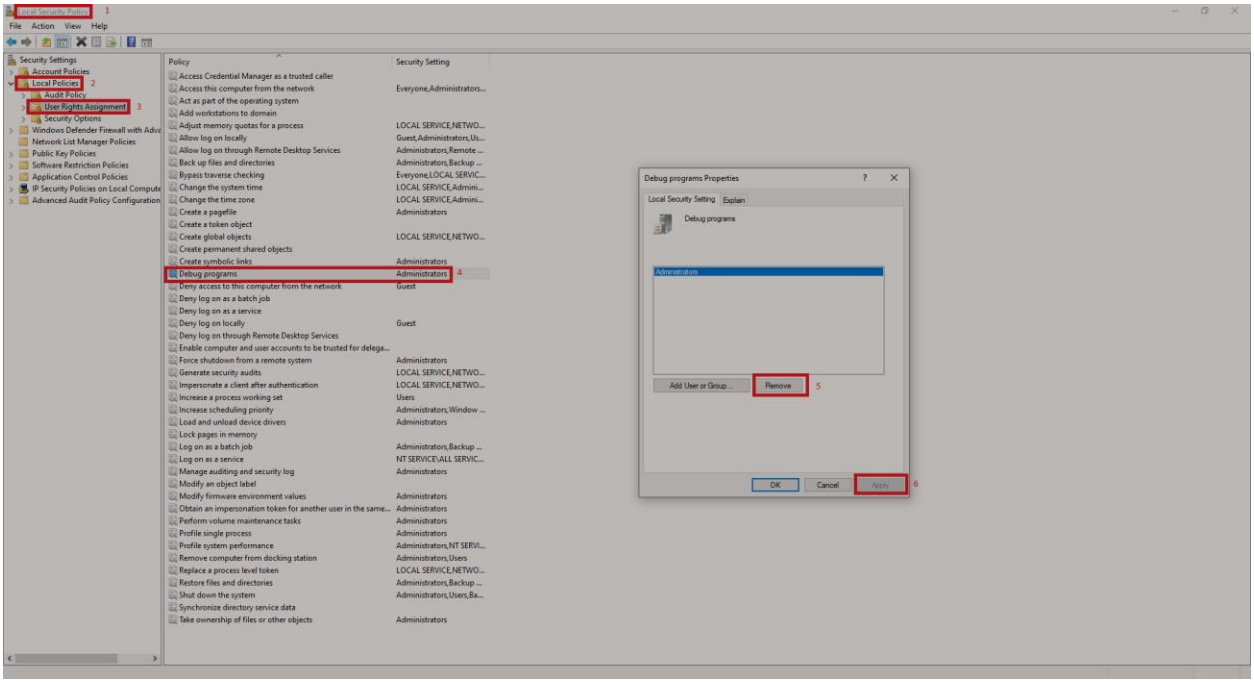
به نام خدا

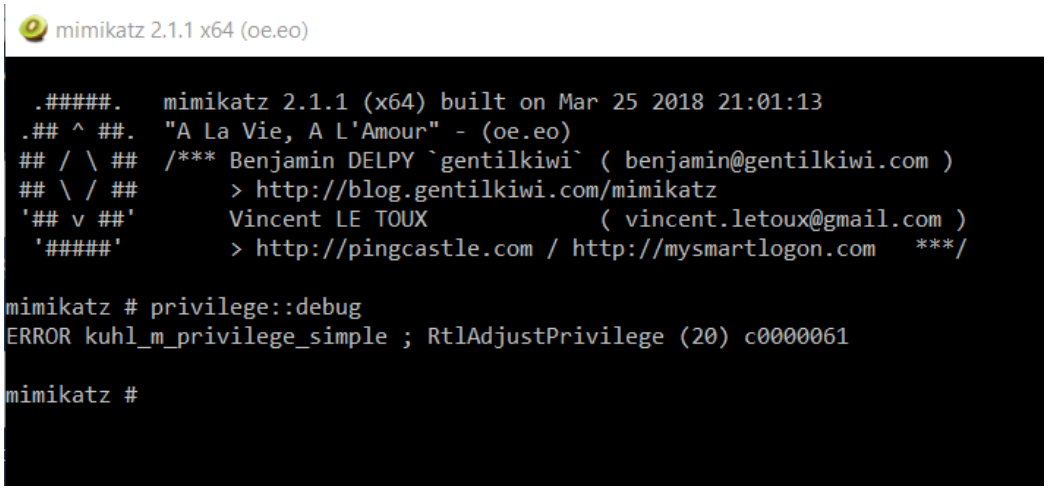
راهکارهای جلوگیری از اجرای Mimikatz روی کامپیوترهای تحت شبکه:

1- **یکی از دسترسی هایی که Mimikatz برای اجرا شدن روی یک کامپیوتر نیاز دارد دسترسی Privilege Debug می باشد تا بتواند پروسه LSASS.EXE را Debug کند. در ویندوز این دسترسی به صورت پیش فرض به Local Administrator داده شده است که جز برای برنامه نویسی سیستمی کاربرد دیگری ندارد و بهتر است دسترسی از این یوزر روی کامپیوتر گرفته شود. برای این کار کنسول Local Security Policy را باز کرده و از با استفاده از مسیر زیر، یوزر administrator را حذف می کنیم:**

Local Policies > User Rights Assignment > Debug programs



با این تنظیمات، مهاجم در صورت اجرای Mimikatz و دستور Privilege::Debug با ارور زیر مواجه می شود:



نکته: مهاجم با استفاده از دستور Privilege::Debug می تواند از دسترسی Local Administrator به Debug Programs مطلع شود.

نکته: توجه کنید که این تنظیم روی سرورهای MSSQL نباید انجام شود و همچنین پیشنهاد می شود این سرورها عضو دامین نباشند.

2- **یکی از دسترسی هایی که Mimikatz برای دسترسی به پسوردهای موجود در پروسه LSASS.EXE به صورت Plain-Text نیاز دارد، روشن بودن پروتکل WDigest می باشد که روی ویندوزهای 8.1 به قبل این پروتکل به صورت پیش فرض روشن می باشد. با وجود آنکه پیشنهاد می شود حتما تمام ویندوزها ورژن 8.1 به بعد باشند اما در صورت لزوم برای استفاده از ویندوزهای ورژن 8.1 به قبل، حتما می بایست این پروتکل را با استفاده از دستور زیر غیر فعال نمود:**

```
reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG_DWORD /d 0
```

با اجرای دستور بالا، اگر مهاجم بتواند Mimikatz را روی کامپیوتر اجرا کند، پسوردها به شکل Hash NTLM نمایش داده خواهد شد.

```
  .#####.   mimikatz 2.1.1 (x64) built on Mar 25 2018 21:01:13
 .## ^ ##.  "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 # privilege::debug
ERROR kuhl_m_privilege_simple ; RtlAdjustPrivilege (20) c0000061

mimikatz # sekurlsa::wdigest
ERROR kuhl_m_sekurlsa_acquireLSA ; Handle on memory (0x00000005)

mimikatz #
```

نکته: مهاجم با استفاده از دستور sekurlsa::wdigest از روشن یا خاموش بودن پروتکل Wdigest رو کامپیوتر قربانی آگاه می شود.

3- **یکی از قابلیت هایی که در ویندوزهای 8.1 به بعد اضافه شده، Lsass Protection می باشد که البته این قابلیت به صورت پیش فرض غیر فعال بوده و می بایست از طریق رجیستری فعال شود. در صورت فعال سازی این قابلیت مهاجم اگر موفق شود روی سیستم Mimikatz را اجرا کند، در مرحله ای که می خواهد Passwordها را خارج کند با ارور مواجه می شود.**

همچنین یکی دیگر از Trickهای مهاجمین استفاده از Lsass Dump می باشد که با ابزارهای مختلفی قابل انجام است و چنانچه قابلیت Lsass Protection روی کامپیوتر فعال شده باشد، مهاجم قادر به Lsass Dump هم نخواهد بود.

با استفاده از دستور زیر قابلیت Lsass Protection فعال می شود:

```
reg add HKLM\SYSTEM\CurrentControlSet\Control\Lsa /v RunAsPPL /t REG_DWORD /d 1
```

```
mimikatz # sekurlsa::logonPasswords
ERROR kuhl_m_sekurlsa_acquireLSA ; Handle on memory (0x00000005)

mimikatz # _
```

نکته: همانطور که اشاره شد، در صورتی که قابلیت Lsass Protection فعال شده باشد، مهاجم در مرحله خارج کردن پسوردها با ارور مواجه می شود.

4- **یکی دیگر از مسائلی که می تواند موجب لو رفتن پسوردهای کامپیوتر توسط مهاجم باشد، سو استفاده از قابلیت Credential Caching می باشد.**

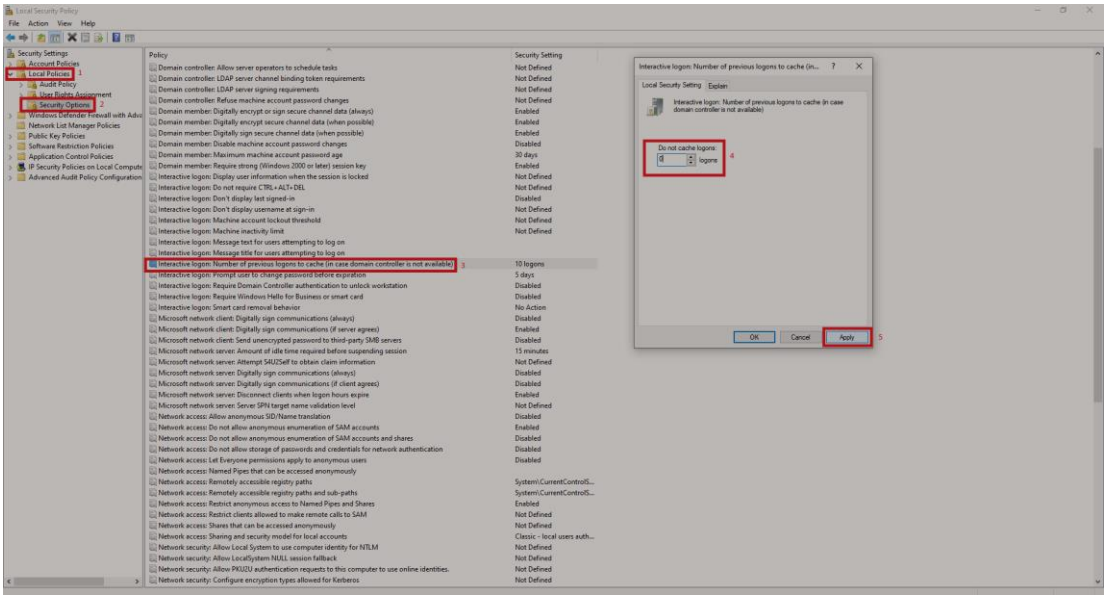
دومین کنترلر به صورت پیش فرض ده پسورد آخر را نگهداری می کند و اگر مهاجم موفق به اجرای Mimikatz روی دومین کنترلر شود، با استفاده از دستور lsadump::cache موفق به استخراج Hash NTLM این پسورها خواهد بود.

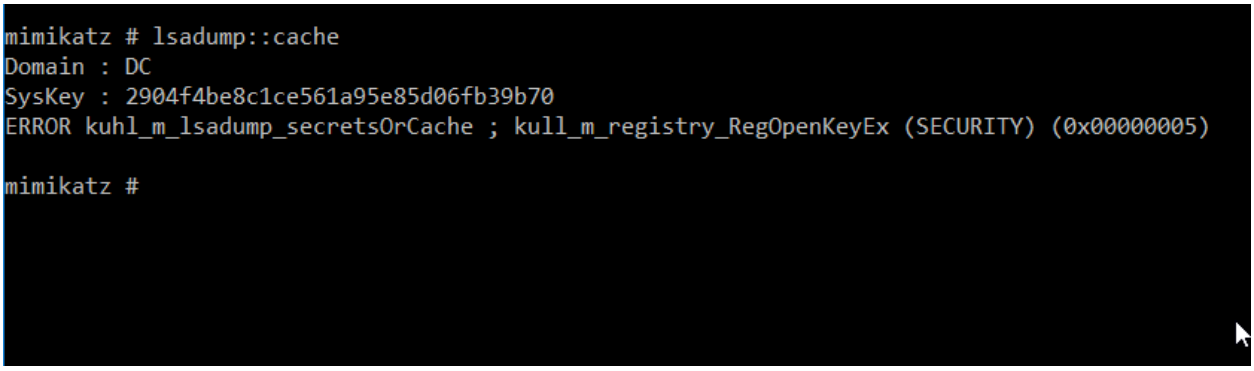
توجه داشته باشید که مهاجم در صورت دستیابی به Hash NTLM پسوردها و با استفاده از سایت https://md5.org قادر به کرک کردن Hash ها خواهد بود (در صورتی که پسوردها از پیچیدگی لازم برخوردار نباشند)

برای غیر فعال کردن Credential Caching کنسول Local Security Policy را باز کرده و با استفاده از مسیر زیر، میزان پسوردی که ویندوز می تواند Cache کند را عدد 0 قرار می دهیم:

Local Policies > Security Options > Interactive Logon: Number of Previous Logons to Cache

دو بار روی Interactive Logon: Number of Previous Logons to Cache کلیک کرده و عدد cache را 0 قرار می دهیم





با 0 کردن Credential Caching و در صورتی که مهاجم موفق به اجرای Mimikatz و دستور lsadump::cache روی کامپیوتر شود با ارور بالا موجه می شود.

5- یکی از راه هایی که مهاجمین برای باقی ماندن در شبکه استفاده می کنند، استفاده از قابلیت Golden Ticket ابزار Mimikatz می باشد. این قابلیت به مهاجم امکان ایجاد یک دسترسی دایمی با گرفتن Golden Ticket را میدهد و به عنوان مثال زمانی هم که ادمین پسورد خود را تغییر دهد، مهاجم با استفاده از Golden Ticket قادر به لاگین کردن روی دامین کنترلر و اجرا دستورات خواهد بود. برای جلوگیری از این موضوع می بایست یوزر krtgbt یا همان Kerberos User روی دامین غیر فعال شود.

لینک های مفید و منبع:

1- Preventing Mimikatz Attacks
2- Configuring Additional LSA Protection
3- How to Mitigate Mimikatz WDigest Cleartext Credential Theft
4- Windows Server: Protected Privileged Accounts
5- Mimikatz - Golden Ticket
6- Kerberos Golden Ticket Protection