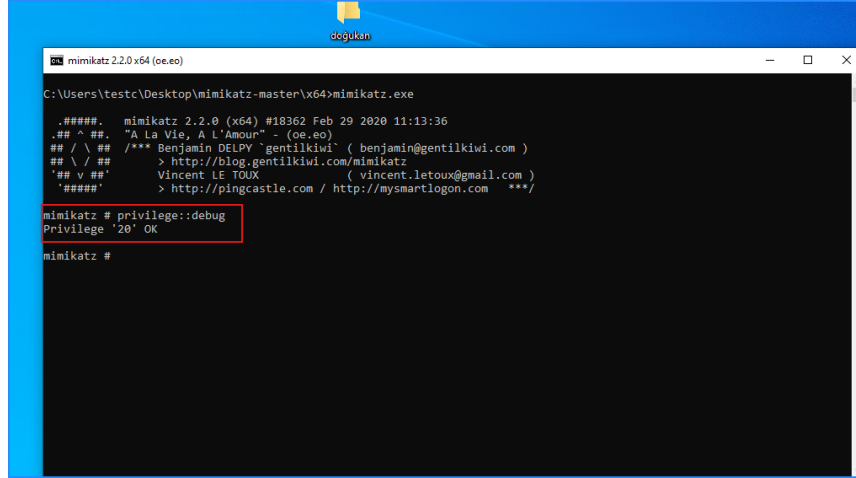


mimikatz Tespiti

mimikatz, hedef Windows 10 makinesine yüklendikten sonra cmd üzerinde “**privilege::debug**” komutu çalıştırılıyor. Bu komut ile Windows sistemdeki kullanıcıya “debug” yetkisi kazandırılıyor. Yani diğer komutların çalışabilmesi için gerekli ayrıcalıkları sağlıyor.



```
C:\Users\testc\Desktop\mimikatz-master\x64>mimikatz.exe

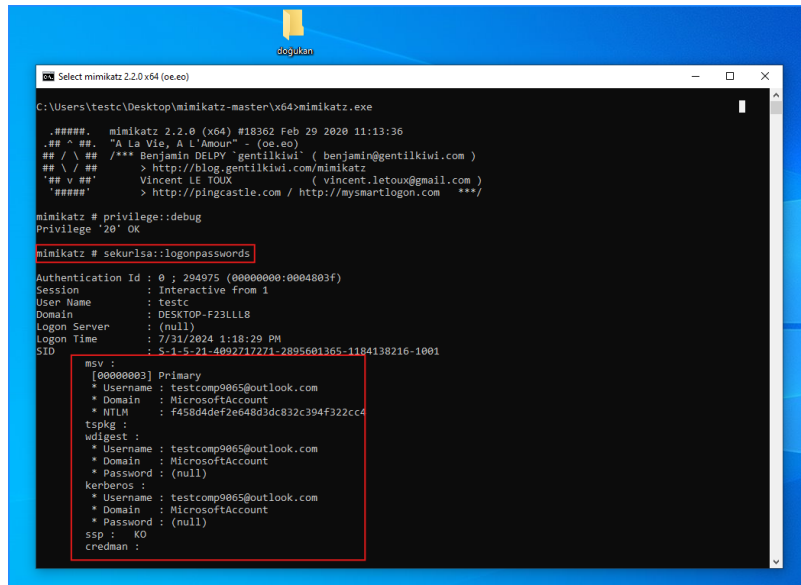
#####.  mimikatz 2.2.0 (x64) #18362 Feb 29 2020 11:13:36
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
## / \ ##  /** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ##   > http://blog.gentilkiwi.com/mimikatz
'## v #'    Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'   > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz #
```

Figure 1 - mimikatz - privilege::debug Komutu

Gerekli ayrıcalıklar alındıktan sonra hedef sistemde mimikatz'in “**sekurlsa::logonpasswords**” komutu çalıştırılıyor. Bu komut ile hedeflenen ise oturum açmış olan kullanıcıların kimlik bilgilerinin (Figure 2) görüntülenmesi oluyor.



```
C:\Users\testc\Desktop\mimikatz-master\x64>mimikatz.exe

#####.  mimikatz 2.2.0 (x64) #18362 Feb 29 2020 11:13:36
.## ^ ##.  "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
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 294975 (00000000:0004803f)
Session           : Interactive from 1
User Name         : testc
Domain           : DESKTOP-F23LL8
Logon Server      : (null)
Logon Time        : 7/31/2024 1:18:29 PM
SID               : S-1-5-21-4092717271-2895681365-1184138216-1001

msv :
[00000003] Primary
* Username : testcomp9065@outlook.com
* Domain   : MicrosoftAccount
* NTLM     : F458d4def2e648d3dc832c394f322cc4
tspkg :
wdigest :
* Username : testcomp9065@outlook.com
* Domain   : MicrosoftAccount
* Password : (null)
kerberos :
* Username : testcomp9065@outlook.com
* Domain   : MicrosoftAccount
* Password : (null)
ssp : KO
credman :
```

Figure 2 - mimikatz - sekurlsa::logonpasswords Komutu

Hedef sistemde komut çalıştırıldıktan sonra Event Viewer üzerinden oluşan loglar incelenerek, komutun çalıştırıldığı saat aralığında Event ID 4688 olan Process Creation log bilgisinin düştüğü görülüyor. Detaylarında çalışan process adı, cmd üzerinde çalıştırılan komutun içeriği, komutu çalıştıran kullanıcı gibi önemli bilgiler yer alıyor.

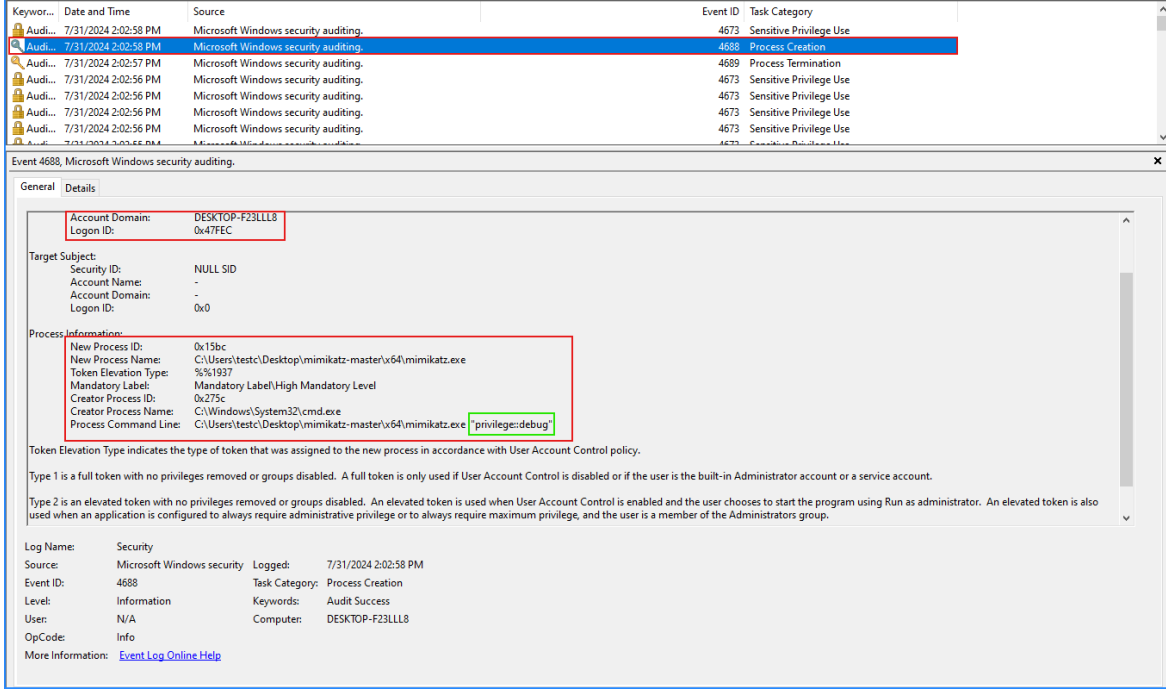


Figure 3 - Event Viewer - 4688 Log Kaydı

mimikatz Sigma Rule

mimikatz ile yapılan saldırılardan korunmak için çeşitli yöntemler mevcuttur. Bunlardan birisi ise bugün ele alınacak olan sigma kurallarıdır. Yazılacak olan sigma kuralını bir SIEM ürünü ile entegre ederek mimikatz aracının yapacağı saldırılar tespit edilip, engellenebilir.

Aşağıda Nextron Systems ailesine ait bir örnek sigma kuralı mevcuttur;

title: Mimikatz Use

id: 06d71506-7beb-4f22-8888-e2e5e2ca7fd8

status: test

description: This method detects mimikatz keywords in different Eventlogs (some of them only appear in older Mimikatz version that are however still used by different threat groups)

references:

<https://tools.thehacker.recipes/mimikatz/modules>

author: Florian Roth (Nextron Systems), David ANDRE (additional keywords)

date: 2017/01/10

modified: 2022/01/05

tags:

- attack.s0002
- attack.lateral_movement
- attack.credential_access
- car.2013-07-001
- car.2019-04-004
- attack.t1003.002
- attack.t1003.004
- attack.t1003.001
- attack.t1003.006

logsource:

product: windows

detection:

keywords:

- 'dpapi::masterkey'
- 'eo.o.e.kiwi'
- 'event::clear'
- 'event::drop'
- 'gentilkiwi.com'
- 'kerberos::golden'
- 'kerberos::ptc'
- 'kerberos::ptt'
- 'kerberos::tgt'
- 'Kiwi Legit Printer'
- 'lsadump::'
- 'mimidrv.sys'
- '\mimilib.dll'
- 'misc::printnightmare'
- 'misc::shadowcopies'
- 'misc::skeleton'

- 'privilege::backup'
- 'privilege::debug'
- 'privilege::driver'
- 'sekurlsa::'

filter:

EventID: 15 # Sysmon's FileStream Events (could cause false positives when Sigma rules get copied on/to a system)

condition: keywords and not filter

falsepositives:

- Naughty administrators
- AV Signature updates
- Files with Mimikatz in their filename

level: high

sekurlsa::logonpasswords Komutu

sekurlsa::logonpasswords, sistemde oturum açmış kullanıcıların bilgilerinin elde edilmesini sağlar. Bu önemli veriler içerisinde kullanıcı adı, domain, NTLM Hash, Kerberos Tickets, Logon type ve zaman bilgileri gibi bilgileri içerir.

LSASS, windows sistemlerde güvenlik politikalarını uygulamak, güvenlik bilgilerini yönetmek ve en önemlisi kimlik doğrulamayı yapmayı sağlayan bir bileşendir. Mimikatz bu komut ile LSASS işleminin belleğine erişim sağlayarak, kritik olan NTLM ve LM hash bilgilerini getirir.